ICS 35.040
L 70

中华人民共和国国家标准

GB/T 18336.3—2001
idt ISO/IEC 15408-3:1999

信息技术　安全技术
信息技术安全性评估准则
第3部分:安全保证要求

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 3:Security assurance requirements

2001-03-08 发布　　2001-12-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等同采用国际标准 ISO/IEC 15408-3:1999《信息技术　安全技术　信息技术安全性评估准则　第3部分:安全保证要求》。

本标准介绍了信息技术安全性评估的安全保证要求。

GB/T 18336 在总标题《信息技术　安全技术　信息技术安全性评估准则》下,由以下3个部分组成:

——第1部分:简介和一般模型

——第2部分:安全功能要求

——第3部分:安全保证要求

本标准的附录A和附录B是提示的附录。

本标准由国家质量技术监督局提出。

本标准由全国信息技术标准化技术委员会归口。

本标准由中国国家信息安全测评认证中心、信息产业部电子第30研究所、国家信息中心、复旦大学负责起草。

本标准主要起草人:吴世忠、吴承荣、龚奇敏、陈晓桦、李守鹏、方关宝、吴亚飞、雷利民、叶红、李鹤田、黄元飞、任卫红。

本标准委托中国国家信息安全测评认证中心负责解释。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构,通过相应组织所建立的涉及技术活动特定领域的委员会参加国际标准的制定。ISO和IEC技术委员会在共同关心的领域里合作,其他与ISO和IEC联盟的政府的和非政府的国际组织也参加了该项工作。

国际标准的起草符合ISO/IEC导则第3部分的原则。

在信息技术领域,ISO和IEC已经建立了一个联合技术委员会——ISO/IEC JTC1。联合技术委员会采纳的国际标准草案交付给国家机构投票表决。作为国际标准公开发表,需要至少75%的国家机构投赞成票。

国际标准ISO/IEC 15408-3是由联合技术委员会ISO/IEC JTC1(信息技术)与通用准则项目发起组织合作产生的。与ISO/IEC 15408-3同样的文本由通用准则项目发起组织作为《信息技术安全性评估通用准则》发表。有关通用准则项目的更多信息和发起组织的联系信息由ISO/IEC 15408-1的附录A提供。

ISO/IEC 15408在"信息技术——安全技术——信息技术安全性评估准则"的总标题下,由以下几部分组成:

第1部分:简介和一般模型

第2部分:安全功能要求

第3部分:安全保证要求

附录A和附录B构成ISO/IEC 15408本部分的提示部分。

以下具有法律效力的提示已按要求放置在ISO/IEC 15408的所有部分:

在ISO/IEC 15408-1附录A中标明的七个政府组织(总称为通用准则发起组织),作为《信息技术安全性评估通用准则》第1至第3部分(称为"CC")版权的共同所有者,在此特许ISO/IEC在开发ISO/IEC 15408国际标准中,非排他性地使用CC。但是,通用准则发起组织在他们认为适当时保留对CC的使用、拷贝、分发以及修改的权利。

中华人民共和国国家标准

信息技术　安全技术
信息技术安全性评估准则
第3部分：安全保证要求

GB/T 18336.3—2001
idt ISO/IEC 15408-3:1999

Information technology—Security techniques—Evaluation criteria for IT security—Part 3:Security assurance requirements

1　范围

本标准定义了保证要求。它包括衡量保证尺度的评估保证级(EAL)、组成保证级的每个保证组件以及PP和ST的评估准则。

1.1　本标准的结构

第1章是本标准的引论和范例。

第3章描述了保证类、子类、组件和评估保证级的表示结构，以及它们之间的关系。同时还刻画了第9章到第15章可找到的保证类和子类的特征。

第4章、第5章和第6章先对PP和ST的评估准则作简要的介绍，然后对在评估中要用到的子类与组件做了详尽的解释。

第7章是评估保证级(EAL)的详尽定义。

第8章对保证类作了简要的介绍，在随后的第9章到第15章给出了这些类的详尽定义。

第16和第17章对保证维护的评估准则做了简要的介绍，其后给出了所用到的子类和组件的详尽定义。

附录A给出了保证组件之间依赖关系的概要。

附录B给出了评估保证级(EAL)和保证组件之间的交叉引用。

1.2　GB/T 18336的保证范例

本条旨在阐述支撑本标准保证方法的基本原则。通过对本条的理解将使读者了解隐含在本标准保证要求中的基本原理。

1.2.1　GB/T 18336基本原则

GB/T 18336的基本原则，就是应该清楚描述那些对安全和组织安全策略承诺所造成的威胁，并且提出足以达到所期望的安全目的的安全措施。

进一步地说，就是应采取一些措施以减少可能存在的脆弱性，减弱有意利用或者无意触发(或利用)一个脆弱性的能力，以及减轻因利用一个脆弱性而导致的破坏程度。另外，还需要采纳一定的措施，便于今后标识一些脆弱性，消除、减轻或通告一个已经被利用或触发过的脆弱性。

1.2.2　保证方法

GB/T 18336的基本原则是为被信任的IT产品或系统的评估(积极的调查)提供保证。评估是提供保证的传统方法，并且是GB/T 18336文档的基础。为了与现行的方法保持一致，GB/T 18336采用相同的基本原则。GB/T 18336建议由专业评估员在不断强调范围、深度和严格性的基础上，衡量文档和已

国家质量技术监督局2001-03-08批准　　2001-12-01实施

完成的IT产品或系统的有效性。

GB/T 18336不排斥也不评论用其他方法的获得保证的有关优点。有关获得安全保证的其他方法还在研究当中。一旦成熟的、可选择的方法产生，可以考虑把它们吸收到GB/T 18336中，因为GB/T 18336的结构允许将来引入更新的内容。

1.2.2.1 脆弱性的意义

假定存在积极寻求违反安全策略的可乘之机的威胁者，他们无论是为了非法获利还是出于别的意图，其行为都是不安全的。威胁者也可能偶然触发了脆弱性，造成对系统的损害。由于处理敏感信息的需求与可用的足够可信产品或者系统缺乏之间的矛盾，一旦IT失效，将会导致很大的风险。因此，破坏IT安全可能造成重大的损失。

破坏IT安全的事件主要发生于应用IT处理业务过程中，脆弱性被有意利用或无意地触发。

应该采取一定的措施防止在IT产品和系统中出现脆弱性。在可行的情况下，脆弱性应该被：

a) 消除——即应该采取积极的措施来发现、除去或者消灭所有可利用的脆弱性；

b) 最小化——即应该采取积极的措施减少任何可利用脆弱性的潜在影响，使残留的脆弱性达到一个可接受的程度；

c) 监视——即应该采取积极的措施，确保发现任何利用残余脆弱性的企图，以便采取及时限制破坏的措施。

1.2.2.2 脆弱性产生的原因

以下的失败可导致脆弱性：

a) 要求——即IT产品或者系统具有所有必要的功能和特性，但仍然可能包含着脆弱性，使得产品或系统在安全方面不合适或者无效；

b) 构造——即IT产品或系统不符合设计规范，或者由于低劣的构造标准或选择了不正确的系统设计而导致了脆弱性；

c) 运行——即IT产品或者系统被正确构造，且符合正确的规范，但是在其运行中由于不适当的控制而导致了脆弱性。

1.2.2.3 本标准的保证

保证是IT产品或系统符合其安全目的的信任基础。保证可从诸如未证实的声明，有关的先期经验，或者特定经验等作参考的原始资料获得。然而，本标准通过积极的调查来提供保证。积极的调查就是对IT产品或者系统进行评估，以确定其安全特性。

1.2.2.4 通过评估获得保证

评估是获取保证的传统手段，并且是GB/T 18336方法的基础。评估技术包括但不限于以下这些：

a) 分析并检查过程和步骤；

b) 检查过程和步骤是否被使用；

c) 分析评估对象(TOE)设计表述之间的一致性；

d) 针对要求分析评估对象(TOE)的设计表述；

e) 验证证据；

f) 分析指导性文档；

g) 分析所开发的功能测试和所提供的结果；

h) 独立的功能测试；

i) 分析脆弱性(包括缺陷假设)；

j) 穿透性测试。

1.2.3 GB/T 18336评估保证尺度

GB/T 18336的基本原则确信，更好的保证源于更大的评估努力，而目标却是运用最小的努力来获得必要的保证级。努力程度的增加基于：

a) 范围——即指，因为包含更多的IT产品或者系统，所以需要更大的努力；

b) 深度——即指，因为要在更好的设计和实施细节这一层次上展开，所以需要更大的努力；

c) 严格性——即指，因为要以更结构化、更形式化的方式应用，所以需要更大的努力。

2 引用标准

下列标准所包括的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型 (idt ISO/IEC 15408-1:1999)

3 安全保证要求

3.1 结构

以下的章条描述了保证类、子类、组件和评估保证级(EAL)的结构，以及它们之间的关系。

图3.1说明了本标准定义的保证要求。注意到，保证要求中最抽象的集合称作一个类。每一个类包含多个保证子类，每一个子类又包含多个保证组件，每一个组件同样又包含多个保证元素。类和子类提供对保证要求进行分类的分类法，而组件用来指明PP和ST中的保证要求。

3.1.1 类结构

保证类的结构如图3.1所示。

3.1.1.1 类名

每一个保证类被指定一个唯一的名字。名字表明保证类涵盖的主题。

保证类名也具有唯一的简洁形式。这是引用保证类的主要的方法。按惯例，采取“A”后跟两个与类名有关的字母。

3.1.1.2 类介绍

每一个保证类有一段介绍，描述类的组成，并且包含了涉及该类意图的支持性文字。

3.1.1.3 保证子类

每一个保证类包含至少一个保证子类。保证子类的结构将在下面的章条中介绍。

3.1.2 保证族结构

保证族的结构如图3.1所示。

3.1.2.1 子类名

每一个保证子类指定一个唯一的名字。该名字描述了与保证子类涵盖的主题相关的信息。每一个保证子类被置于一个保证类之内，这个保证类也包括具有相同意图的其他保证子类。

保证子类名也有一个唯一的简洁形式，这是引用保证子类的主要方法。按惯例，其表示方法是所在类名的缩写，加下划线，然后再加上与子类名有关的三个字母。

3.1.2.2 目的

保证子类的目的部分说明保证子类的意图。

这部分描述了该保证子类所要表明的目的，特别是那些与GB/T 18336保证范例有关的目的。这个保证子类的描述是一般的描述。目的所要求的任何特定细节都应包含在该保证组件中。

3.1.2.3 组件分级

每一个保证子类包含一个或多个保证组件。保证子类的这一部分主要描述可供使用的组件并且解释它们之间的差异。一旦确定该保证子类对PP/ST保证要求而言是必需或是有用的部分，就要区分这些保证组件，这是组件分级的主要目的。

含有超过一个组件的保证子类将被分级并说明分级的理由。分级将依据范围、深度或者严格性的原则进行。

3.1.2.4 应用注释

如果有应用注释部分的话，它将提供这个保证子类的附加信息，而这些信息应该是保证子类用户（例如 PP 和 ST 的作者、TOE 的设计者、评估者等等）特别感兴趣的。它的表示是非形式化的，并且包括限制使用的警告和特别要注意的地方。

3.1.2.5 保证组件

每一个保证子类至少有一个保证组件。保证组件的结构将在下一条描述。

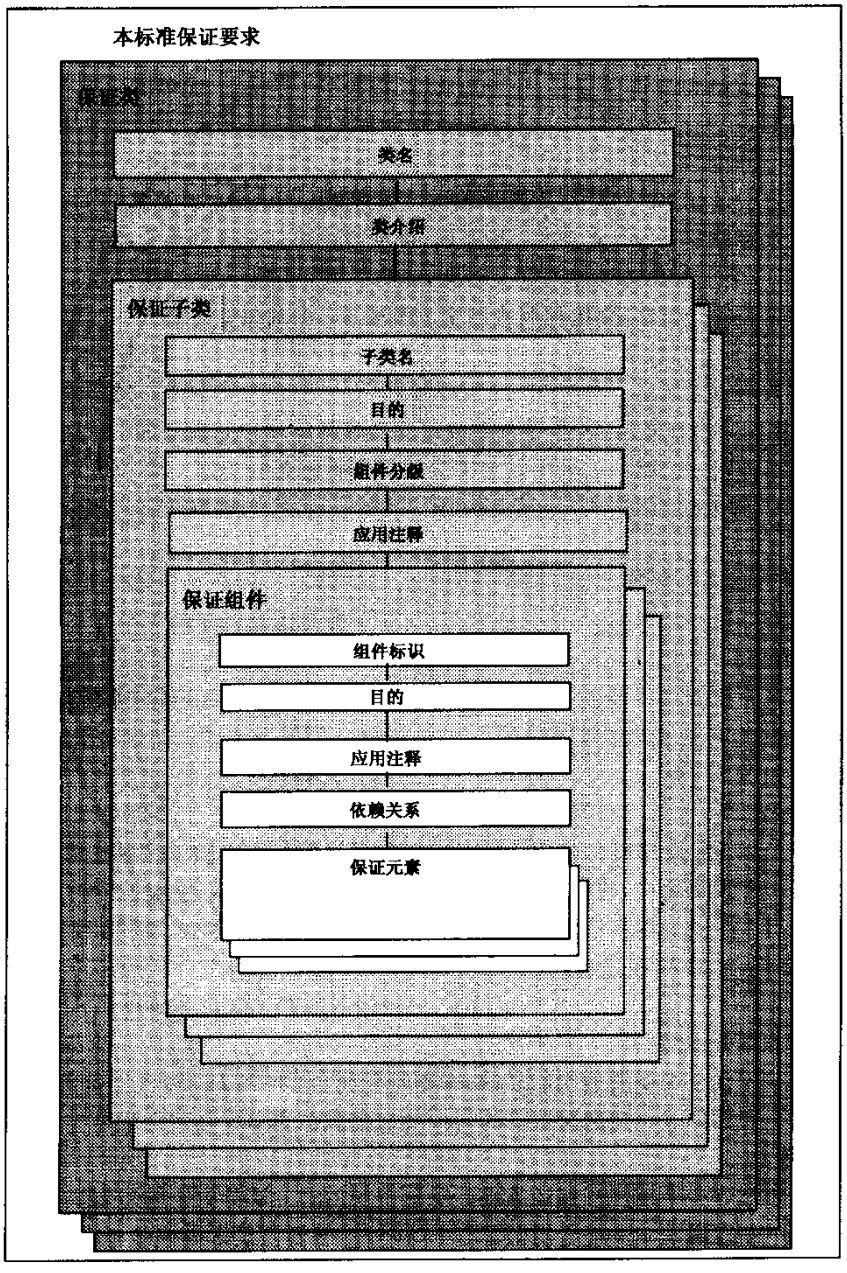

图 3.1 保证类/子类/组件/元素的层次

3.1.3 保证组件结构

保证组件的结构如图 3.2 所示。

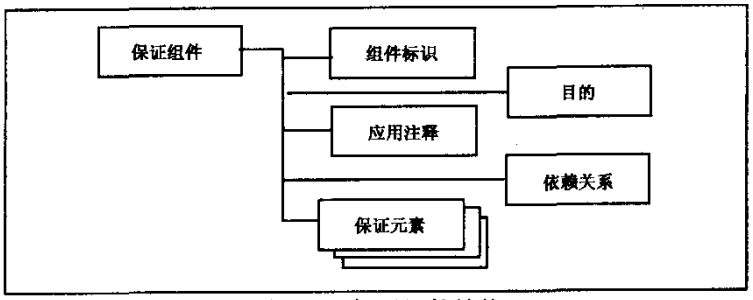

图 3.2 保证组件结构

保证子类内组件之间的关系用粗体突出表示。那些新的要求，连同对同一级内前面组件的增强或修改部分，也用粗体突出表示。对于依赖关系也同样用粗体突出表示。

3.1.3.1 组件标识

组件标识部分给出一些描述信息，这些信息对标识、分类、登记和引用一个组件是必须的。

每个保证组件指定唯一的一个名字。该名字提供关于该保证组件所涉及主题的描述性信息。每个保证组件均放置在与其共享安全目的的保证子类之内。

保证组件名字也给定了唯一的简洁形式，这是引用保证组件的主要方法。按惯例，简洁形式为子类名的缩写，后面加一个点，然后是数字符号。这个数字符号是根据组件在子类内的顺序从 1 开始编号的。

3.1.3.2 目的

如果保证组件有目的部分，那么它包含了特定保证组件的特定目的。在含有这部分信息的保证组件中，该信息详尽地解释了该组件的特定意图和目的。

3.1.3.3 应用注释

如果保证组件有应用注释部分，则它包含了一些附加的信息，以便于使用该组件。

3.1.3.4 依赖关系

当一个组件无法自我满足而依赖于另一个组件时，依赖关系就出现在这些保证组件中。

每一个保证组件都给出了一个完整的列表，表明了它与其他保证组件的依赖关系。一些组件可能“无依赖关系”，这表明它没有依赖于其他组件。被依赖的组件也可能依赖于其他组件。

依赖关系列表标识了所依赖的保证组件的最小集合。在依赖关系列表中与另一组件同层次的组件也可以用来满足依赖关系。

在特殊情况下，所表明的依赖关系可能并不适用。PP/ST 的作者可以提供为什么给定的依赖关系不适用的理由，并选择不去满足这种依赖关系。

3.1.3.5 保证元素

每一个保证组件给出了一组保证元素。一个保证元素就是一个安全要求，如果进一步细分的话，这个安全要求不会产生有意义的评估结果。它是本标准中最小的安全要求。

每一个保证元素都被确定属于以下三组保证元素中的一组：

a) 开发者行为元素：即由开发者将实施的活动。这组行为靠下一组元素中引用的证据材料来证明是否合格。开发者行为要求用元素编号上附加一个字母“D”的方法来表示。

b) 证据的内容和形式元素：即所要求的证据、证据所显示的以及证据所表述的信息。证据的内容和形式要求用元素编号上附加字母“C”的方法来表示。

c) 评估者行为元素：即评估者实施的活动。这组行为隐含了对在前面两组元素中规定要求的证实，并且隐含了除开发者实施的活动之外还须实施的行为或分析。评估者行为要求用元素号上附加字母“E”的方法来表示。

开发者行为与证据内容和形式这两组元素定义了代表一个开发者职责的保证要求，而该开发者的职责就是论证 TOE 的安全功能保证。通过满足这些要求，开发者能够更加确信 TOE 满足 PP 或 ST 的功能和保证要求。

评估者行为从评估的两个方面明确了评估者的责任。一个方面是根据第 5 章和第 6 章中定义的 APE 和 ASE 来确认 PP/ST，另一方面是验证 TOE 与其功能和保证要求的一致性，通过证明 PP/ST 是有效的并且 TOE 满足这些要求，评估者可以提供一个信任的基础，确信这个 TOE 满足其安全目的。

评估者行为元素结合了证据的内容和形式，指明了在验证 TOE 的 ST 中所作的安全声明时将要进行的评估活动。

3.1.4 保证元素

每一个元素代表一个需要满足的要求。描述要求的语句应当清晰、简洁且无歧义。因此，不能出现复杂句式，即每一可分离的要求将作为单独的元素来说明。

对于使用的术语，元素采用常见辞典上的意思，而不采用那些预先规定的术语的缩写形式，因为那将导致隐含性要求。因此，元素都表述为明确的要求，而不用保留术语。

与 GB/T 18336 第 2 部分不同之处在于，在本标准中没有与元素有关的赋值和选择操作。然而，本标准可能根据需要进行“细化”操作。

3.1.5 EAL 结构

图 3.3 说明了在本标准中定义的所有评估保证级(EAL)和相应的结构。注意，图中显示出保证组件的内容的同时，还将通过引用 GB/T 18336 中定义的实际组件来将该结构信息包含在一个评估保证级(EAL)中。

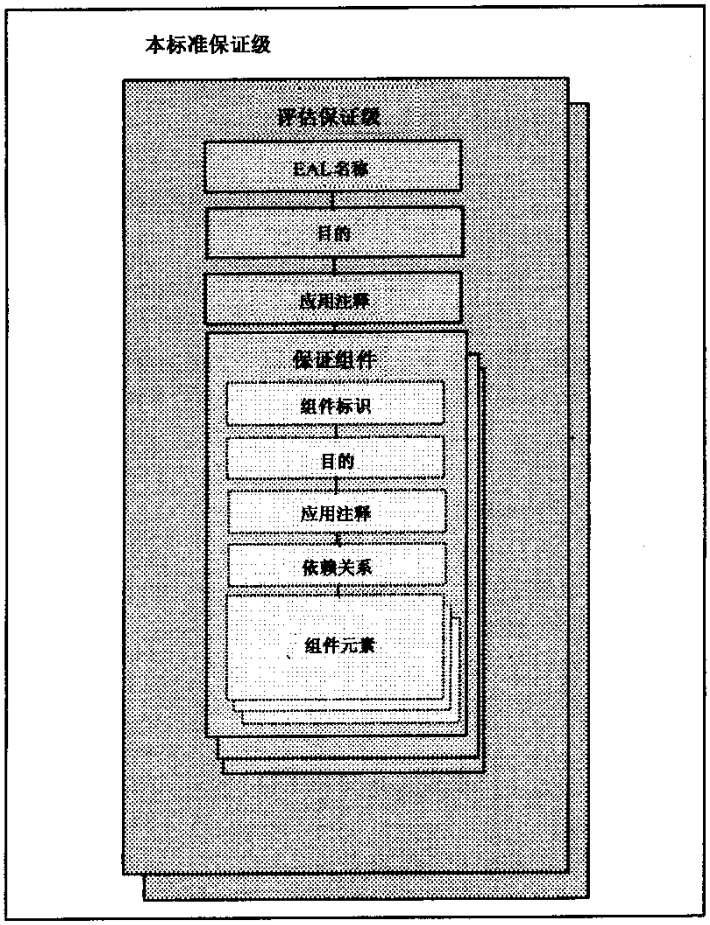

图 3.3 EAL 结构

3.1.5.1 EAL 名称

给每一评估保证级(EAL)指定唯一的名称。该名称提供关于评估保证级(EAL)意图的描述性信息。

评估保证级(EAL)名称有唯一的简洁形式,这是引用评估保证级(EAL)的主要方法。

3.1.5.2 目的

评估保证级(EAL)的目的部分表明了评估保证级(EAL)的意图。

3.1.5.3 应用注释

如果评估保证级(EAL)有应用注释部分,则它包含评估保证级(EAL)的使用者(如 PP 和 ST 的作者、以该评估保证级(EAL)为目的的评估对象(TOE)的设计者、评估者) 特别感兴趣的信息。它的表示是非形式化的,并且包含了限制使用的警告和应特别注意的地方。

3.1.5.4 保证组件

必须为每一个评估保证级(EAL) 选择一组保证组件。

可以用以下方法,得到一个比给定的评估保证级(EAL)所提供的保证具有更高级别的保证:

a) 从其他保证子类中选取额外的保证组件;

b) 从相同的保证子类中用更高级别的保证组件替换该保证组件。

3.1.6 保证和保证级的关系

图 3.4 说明了本标准定义的保证要求和保证级之间的关系。当保证组件进一步分解为保证元素时,保证元素不能被保证级单独引用。注意,图中的箭头表示从一个评估保证级(EAL)到其所在类中一个保证组件的引用。

3.2 组件分类

本标准包含一些根据相关保证分组的子类和组件的类。在每一个类的开始是一个图表,指出该类中的子类和子类中的组件。

在图 3.5 中,所显示的类包含一个单一的子类。这个子类包含三个线性分级的组件(如组件 2 在特定行为、特定证据以及在行为或证据的严格性等方面上比组件 1 要求得更多)。在本标准中的保证子类都是线性分级的,尽管"线性" 对以后可能增加的保证子类而言,并不是的一个强制性的准则。

3.3 保护轮廓(PP)和安全目标(ST)评估准则类的结构

保护轮廓(PP)和安全目标(ST)的评估要求被视为保证类,并且被表示为与其他保证类相似的结构,而这些结构将在下面进行描述。值得注意的是,相关的子类描述中没有组件分级这一部分。这是因为每一个子类仅仅有单一的组件,没有分级的情况。

在本标准的第 4 章,表 4.1、4.2、4.3 和 4.4 概述了组成 APE 类和 ASE 类的子类以及两类的缩写。有关 APE 类中子类的叙述概要见 GB/T 18336 第 1 部分附录 B 的 B2.2 到 B2.6,有关 ASE 类中子类的叙述概要见 GB/T 18336 第 1 部分附录 C 的 C2.2 到 C2.8。

3.4 本标准中术语的应用

以下是本标准需要准确使用的术语列表,它们并非对术语表的内容有任何扩充,因为它们只是一般词语,它们的用法尽管被以下的定义所限制,但仍然和词典中的意思一致。然而,这些术语曾作为本标准开发的指导,因此有助于一般性的理解。

3.4.1 检查 check

这个术语类似于"确认"或者"验证",但是并没有那么严格。这个术语要求评估者在经过一个粗略的分析,或者根本没有分析的情况下迅速作出决定。

3.4.2 连贯 coherent

一个逻辑上有序的实体具有可辨别的意义。对于文档,这意味着既表示文档的实际文本又表示文档的结构,取决于它是否能为读者所理解。

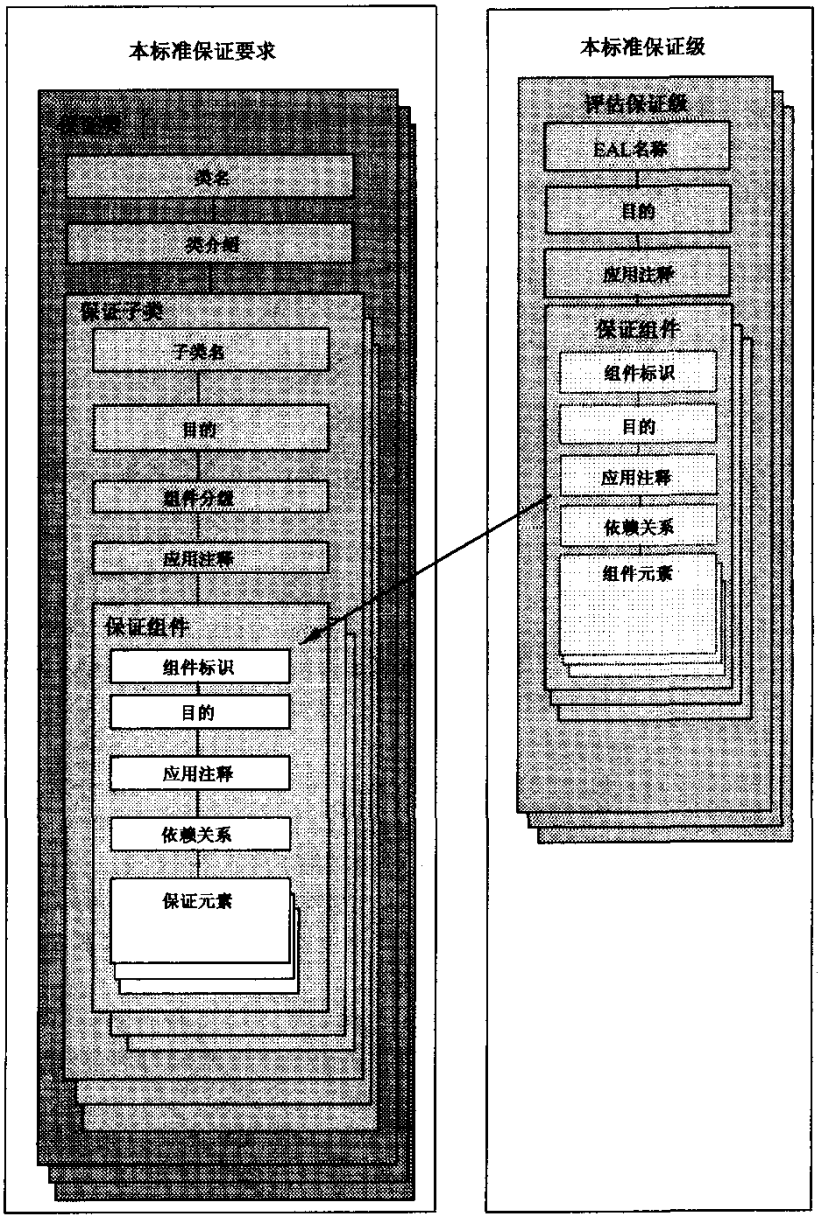

图 3.4 保证和保证级的关系

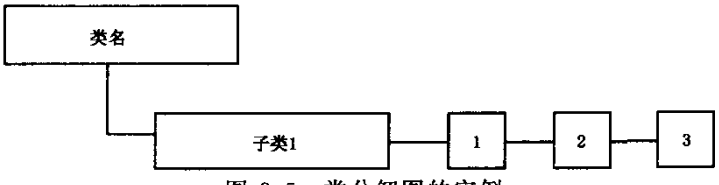

图 3.5 类分解图的实例

3.4.3 完备 complete

提供一个实体所有必要的部分。用在文档中，这意味着该文档包含所有信息，其详细程度应达到一定的水平，在这个抽象程度的水平上不再需要进一步解释了。

3.4.4 确认 confirm

这个术语用来表明某些事情需要在细节上进行复查，并且需要对其充分性作出独立的判断。严格的程度取决于主体本身的性质。这个术语仅适用于评估者行为。

3.4.5 一致 consistent

这个术语描述两个或者更多实体之间的关系，表明这些实体之间没有明显的矛盾。

3.4.6 对抗 counter

这个术语主要表示一个安全对象对抗了一个特殊的威胁，但是不需要指出威胁最终被完全根除。

3.4.7 论证 demonstrate

这个术语指一个可得出结论的分析，它不如“严格证明”严格。

3.4.8 描述 describe

这个术语要求提供一个实体确定的特定细节。

3.4.9 决定 determine

这个术语要求作出独立的分析，以获得一个特定的结论。这个术语的用法不同于“确认”或者“验证”，因为后两者意味着分析已经完成而只需要复查，而“决定”意味着通常在没有进行任何分析的情况下作出一个真正独立的分析。

3.4.10 确保 ensure

这个术语意味着行为和结果之间有很强的因果关系。该术语典型的用法是把“帮助”加在前面，表明它仅仅基于行为，而不是对结果的充分肯定。

3.4.11 彻底 exhaustive

这个术语在本标准中表明实施分析或者其他行为。它与“系统的”有关，但是相对更强一些。它表明，不仅要根据一个明确的计划采取系统化的方法实施分析或其他行为，而且其后的计划应足以保证所有可能的方法都已被采纳了。

3.4.12 解释 explain

这个术语不同于“描述”和“论证”。它旨在回答“为什么?”，而并非试图争辩所采取行动的过程是最佳的。

3.4.13 内在一致 internally consistent

实体的任何方面之间没有明显的矛盾。在文档中，这意味着没有自相矛盾的地方。

3.4.14 证明 justification

这个术语指用于得出结论的分析，但是比“论证”更严格。这个术语要求，在非常仔细和彻底地解释逻辑论点的每一个步时都需十分严格。

3.4.15 相互支持 mutually supportive

这个术语描述一组实体之间的相互关系，表明实体占有的资源不与其他实体相冲突，甚至可能辅助其他的实体完成任务。它并不需要判断所有有关的独立实体是否直接支持所在组中的其他实体，而是一个更具一般意义的判断。

3.4.16 严格证明 prove

这指在数学意义上的一个形式化分析。它的各个方面完全都是严格的。典型地讲，“严格证明”主要用于在高级别严格性的情况，以显示两个 TSF 表示之间的对应关系。

3.4.17 规定 specify

这个术语的使用情况与“描述”一样，但是倾向更严格和准确的含义。它十分类似于“定义”。

3.4.18 追溯 race

这个术语用来表明在具有最小级别严格性的两个实体之间所要求的一种非形式化的对应。

3.4.19 验证 verify

这个术语的用法类似于“确认”，但是有更严格的含义。当这个术语用于评估者行为时，表明要求评

估者独立地作出努力。

3.5 保证分类

保证类、子类和每一个保证子类的缩写在表 3.1 中进行说明。

表 3.1 保证子类细目分类和对应关系

保证类	保证子类	缩写名称
·ACM 类:配置管理	CM 自动化	ACM _ AUT
	CM 能力	ACM _ CAP
	CM 范围	ACM _ SCP
ADO 类:交付和运行	交付	ADO _ DEL
	安装、生成和启动	ADO _ IGS
ADV 类:开发	功能规范	ADV _ FSP
	高层设计	ADV _ HLD
	实现表示	ADV _ IMP
	TSF 内部	ADV _ INT
	低层设计	ADV _ LLD
	表示对应性	ADV _ RCR
	安全策略模型	ADV _ SPM
AGD 类:指导性文档	管理员指南	AGD _ ADM
	用户指南	AGD _ USR
ALC 类:生命周期支持	开发安全	ALC _ DVS
	缺陷纠正	ALC _ FLR
	生命周期定义	ALC _ LCD
	工具和技术	ALC _ TAT
ATE 类:测试	覆盖范围	ATE _ COV
	深度	ATE _ DPT
	功能测试	ATE _ FUN
	独立性测试	ATE _ IND
AVA 类:脆弱性评定	隐蔽信道分析	AVA _ CCA
	误用	AVA _ MSU
	TOE 安全功能强度	AVA _ SOF
	脆弱性分析	AVA _ VLA

3.6 保证类和子类概况

以下是对第 9 章至第 15 章的保证类和子类的概述。这些类和子类的概述是按第 9 章到第 15 章类和子类出现的顺序排列的。

3.6.1 ACM 类:配置管理

配置管理(CM—Configuration Management)通过在细化和修改 TOE 及其他有关信息的过程中进行规范和控制,确保 TOE 的完整性。配置管理(CM)阻止对 TOE 进行非授权的修改、添加或删除,这保证了用于评估的 TOE 和文档确是准备交付的 TOE 和文档。

3.6.1.1 CM 自动化(ACM _ AUT)

配置管理自动化对一些配置项的控制实现了一定程度的自动化。

3.6.1.2 CM 能力(ACM _ CAP)

配置管理能力定义了配置管理系统的一些特性。

3.6.1.3 CM 范围(ACM _ SCP)

配置管理范围指出了需要由配置管理系统控制的 TOE 项目。

3.6.2 ADO 类:交付和运行

保证类 ADO 定义了有关安全交付、安装、运行 TOE 的措施、程序和标准的要求,以确保 TOE 提供的安全保护在传递、安装、启动和运行时不会被削弱。

3.6.2.1 交付(ADO _ DEL)

交付包含了将 TOE 传递给用户的过程中用以维护其安全性的程序,既包含初始的交付,也包含后来的修改。它还包括了用来论证已交付的 TOE 真实性的特殊程序或操作。这些程序和措施是确保 TOE 提供的安全保护没有在传递过程中被削弱的基础。尽管在评估一个 TOE 时,并非总是能够决定其是否遵照了交付要求,但总是能够对开发者开发的将 TOE 交付给用户的程序进行评估。

3.6.2.2 安装、生成和启动(ADO _ IGS)

安装、生成和启动需要管理员配置和激活 TOE 的拷贝,以显示它与 TOE 的主拷贝有相同的保护特性。安装、生成和启动程序需要确信管理员明白配置参数以及它们对 TSF 的影响。

3.6.3 ADV 类:开发

保证类 ADV 定义了 ST 中从 TOE 概要规范到实际 TSF 的逐步细化的一系列要求。每一个产生结果的 TSF 表示都提供信息,以帮助评估者决定 TOE 的功能要求是否被满足了。

3.6.3.1 功能规范(ADV _ FSP)

功能规范描述了 TSF,而且它一定是 TOE 安全功能要求的一个完整而准确的实例化。功能规范也详细描述了 TOE 的外部接口。TOE 的用户希望通过此接口同 TSF 交互信息。

3.6.3.2 高层设计(ADV _ HLD)

高层设计是一个顶层的设计规范,它将 TSF 功能规范细化成 TSF 的一些组成部分。高层设计指明了 TSF 的基础结构和主要的硬件、固件和软件元素。

3.6.3.3 实现表示(ADV _ IMP)

实现表示是 TSF 具体的表示。它根据可用的源代码、硬件图详细表述了 TSF 的内部工作方式。

3.6.3.4 TSF 内部(ADV _ INT)

TSF 内部要求指明了 TSF 必需的内部结构。

3.6.3.5 低层设计(ADV _ LLD)

低层设计是具体化的设计规范,它将高层设计细化成具体的一层,作为编程或硬件构造的基础。

3.6.3.6 表示对应性(ADV _ RCR)

表示对应性论证了所有相邻的从 TOE 概要规范到所提供的具体 TSF 表示相邻对之间的映射关系,这些表示对包括。

3.6.3.7 安全策略模型(ADV _ SPM)

安全策略模型是 TSP 安全策略的结构化描述,保证功能规范和 TSF 的安全策略相符合,并且最终和 TOE 的安全功能要求相符合。这是通过功能规范、安全策略模型和模型化的安全策略之间的对应来实现的。

3.6.4 AGD 类:指导性文档

保证类 AGD 从开发者提供的可操作文档的易懂性、覆盖范围和完整性等方面定义了指导性要求。该文档提供两种类型的信息,一类是针对用户,另一类针对管理员,这是 TOE 安全运行的一个重要因素。

3.6.4.1 管理员指南(AGD _ ADM)

管理员指南的要求有助于 TOE 的管理员和操作员理解环境的限制。管理员指南是开发者可用的主要方法，便于为 TOE 管理员提供如何安全地管理 TOE 和如何高效地利用 TSF 的优点和保护功能等详细准确的信息。

3.6.4.2 用户指南(AGD_USR)

用户指南的要求有助于用户能够安全地运行 TOE(如，必须清楚地解释和说明 PP 或 ST 所假设的使用限制)。用户指南是开发者可用的主要方法，便于为 TOE 用户提供必要的背景知识以及如何正确使用 TOE 的保护功能这一特定信息。用户指南必须包含两方面的内容：首先，它必须解释那些用户可见的安全功能的目的以及如何使用它们，这样用户可以持续有效地保护他们的信息；其次，它必须解释在维护 TOE 的安全时用户所起的作用。

3.6.5 ALC 类：生命周期支持

保证类 ALC，通过采用一个为 TOE 开发的所有步骤定义的生命周期模型，明确了保证要求。这个生命周期包括纠正缺陷的程序和策略，以及保护开发环境的工具、技术和安全措施的正确使用。

3.6.5.1 开发安全(ALC_DVS)

开发安全涉及在开发环境中使用的物理上的、程序上的、人员上的和其他方面的安全措施。它包括开发场所的物理安全和对开发人员的选择和雇用的控制。

3.6.5.2 缺陷纠正(ALC_FLR)

缺陷纠正确保开发者维护 TOE 时，将记录和纠正由 TOE 用户发现的缺陷。但是在评估 TOE 时，无法判断将来是否仍遵从缺陷纠正的要求，因而有可能对开发者已有的用来跟踪、修补缺陷和交付补丁给用户的程序和策略进行评估。

3.6.5.3 生命周期定义(ALC_LCD)

生命周期定义表明，开发者用以制造 TOE 的工程实践包括在开发过程和运行维护要求中已明确的设想和活动。当安全分析和证据生成作为开发过程和运行维护活动中的一个完整的部分且按照正规的方式实施时，就将提高安全要求和 TOE 之间的对应性的信任度。本组件的目的不是规定任何特定的开发过程。

3.6.5.4 工具和技术(ALC_TAT)

工具和技术指出，需要定义一些用于分析和实现 TOE 的开发工具。它包括与开发工具有关的要求，以及依赖于这些所选择工具的 TOE 实现的要求。

3.6.6 ATE 类：测试

保证类 ATE 陈述了论证 TSF 满足 TOE 安全功能要求的测试要求。

3.6.6.1 覆盖范围(ATE_COV)

覆盖范围涉及开发者针对 TOE 而进行功能测试的完整性。它描述了所要测试的 TOE 安全功能的范围。

3.6.6.2 深度(ATE_DPT)

深度涉及开发者测试 TOE 的详细程度。安全功能测试是根据从 TSF 表示的分析中得出的信息，逐步增加其深度而进行的测试。

3.6.6.3 功能测试(ATE_FUN)

功能测试表明，TSF 表现出满足 ST 要求所需的特性。功能测试提供了 TSF 应满足所选功能组件最低要求的保证。然而功能测试并没有规定 TSF 不会超过最低的要求。这个子类的重点在于开发者自己进行的功能测试。

3.6.6.4 独立性测试(ATE_IND)

独立性测试规定 TOE 的功能测试必须由一个除开发者之外的团体(如，第三方)实施。这个子类通过引入非开发者所进行的测试来提高其使用价值。

3.6.7 AVA 类：脆弱性评定

保证类 AVA 定义了有关标识可利用的脆弱性的指导性要求。特别地，它指出了在构造、运行、误用或错误配置 TOE 时引入的脆弱性。

3.6.7.1 隐蔽信道分析(AVA_CCA)

隐蔽信道分析主要用来发现和分析未预料到的一些通信信道，这些通信信道可用来违背预期的 TSP。

3.6.7.2 误用(AVA_MSU)

误用分析将考察管理员或用户在理解指导性文档后，能确定 TOE 是否以不安全的方式被配置和运行。

3.6.7.3 TOE 安全功能强度(AVA_SOF)

功能强度分析说明了以概率或排列机制(如，口令字或哈希函数)实现的 TOE 安全功能。即使不会避开它，使其无效或破坏它，仍然可用直接攻击的办法来击败它。对于每个功能强度可以要求一个级别或一个特殊的量度。实施功能强度分析的目的就是判断该功能是否满足或超出了这个要求。例如，对口令机制的功能强度分析可以通过说明口令空间有足够大来指出口令字功能满足强度要求。

3.6.7.4 脆弱性分析(AVA_VLA)

脆弱性分析包括标识在开发过程的不同细化步骤引入的潜在缺陷。它通过收集以下有关的必要信息来导出穿透性测试的定义：(1)TSF 的完备性(该 TSF 是否可以抵抗所有假设的威胁?)；(2)所有安全功能之间的依赖关系。这些潜在的脆弱性将通过穿透性测试来评估，以判断它们在实际应用中是否会被利用来削弱 TOE 的安全。

3.7 维护分类

对保证维护的要求也视为一个保证类，并且也用以上的类结构来定义。

这些保证维护子类和每个子类的缩写见表 3.2。

表 3.2 保证维护类分解

保证类	保证子类	缩写
保证维护	保证维护计划	AMA_AMP
	TOE 组件分类报告	AMA_CAT
	保证维护证据	AMA_EVD
	安全影响分析	AMA_SIA

3.8 保证维护类和子类概况

下面概括第 17 章的保证类和子类。这些类和子类的概要的顺序同第 17 章出现的顺序相同。

3.8.1 AMA 类：保证维护

保证类 AMA 的目的是维护保证级，即当 TOE 或其环境发生改变时，TOE 可以继续满足它的安全目标。在这个类中的每个子类都标识了在成功地评估 TOE 之后，开发者和评估者应实施的行为，虽然有些要求可能是在评估的时候已经进行了。

3.8.1.1 保证维护计划 (AMA_AMP)

保证维护计划确定了开发者将实施的计划和程序，其目的就是当 TOE 或其环境改变时，可以确保评估过的 TOE 所建立的保证得到维护。

3.8.1.2 TOE 组件分类报告 (AMA_CAT)

根据 TOE 组件(如，TSF 子系统)相对于安全的重要性，对 TOE 组件分类的报告提供了对它们进行分类的方法，这个分类将作为开发者进行安全影响分析的重点。

3.8.1.3 保证维护证据 (AMA_EVD)

保证维护证据旨在寻求建立一种信任关系，以确保开发者将根据保证维护计划来维护 TOE。

3.8.1.4 安全影响分析（AMA _ SIA）

安全影响分析旨在寻求建立一种信任关系，以确保 TOE 经过评估之后，开发者将分析所有的变化对 TOE 的安全影响来维护对 TOE 的保证。

4 保护轮廓与安全目标评估准则

4.1 概述

本章介绍 PP 和 ST 的评估准则。这些评估准则将在第 5 章“APE 类：保护轮廓评估”和第 6 章“ASE 类：安全目标评估”中进一步详细阐述。

这些准则在本标准中是首要的，因为 PP 和 ST 评估通常是在 TOE 评估之前进行的。它们在评定 TOE 以及评估功能和保证要求时起着特殊的作用，以便证明 PP 和 ST 对 TOE 评估来说是否是一个有意义的基础。

虽然这些评估准则与第 8 章至第 15 章的要求稍有差异，但它们却十分相似，因为就 PP、ST 和 TOE 评估而言，开发者和评估者的行为是可以类比的。

PP 类、ST 类与 TOE 类不同，因为 PP 类和 ST 类的所有要求都要考虑单个 PP 和 ST 的评估，而 TOE 类的要求则涉及一个较为广泛的论题，但并非要对一个给定的 TOE 考虑所有的论题。

PP 和 ST 的评估准则的基础是 GB/T 18336 第 1 部分附录 B 和附录 C 所提供的信息。其中可以找到关于 APE 和 ASE 类要求的有用的背景信息，这在以下的章条中也有描述。

4.2 保护轮廓准则概述

4.2.1 保护轮廓评估

PP 评估的目的是为了论证 PP 是完备的、一致的，技术上是合理的，因此适合作为一个或多个可评估 TOE 的要求陈述。这样的 PP 符合注册的条件。

4.2.2 与安全目标评估准则的关系

正如 GB/T 18336 第 1 部分附录 B 和附录 C 所描述的一样，在通常的 PP 和具有 TOE 特性的 ST 之间，有着许多结构和内容上的相似之处。因此，PP 评估准则包含的要求与 ST 评估准则包含的要求之间有许多相似之处，并且二者的表示方式也相似。

4.2.3 评估者任务

4.2.3.1 仅仅基于 GB/T 18336 要求评估的评估者的任务

评估者实施一个包含在 GB/T 18336 要求之内的 PP 评估时，应当使用表 4.1 列出的 APE 类的要求。

表 4.1 保护轮廓子类—仅用 GB/T 18336 的要求

类	子类	缩写
APE 类：保护轮廓评估	保护轮廓，TOE 描述	APE _ DES
	保护轮廓，安全环境	APE _ ENV
	保护轮廓，PP 引言	APE _ INT
	保护轮廓，安全目的	APE _ OBJ
	保护轮廓，IT 安全要求	APE _ REQ

4.2.3.2 GB/T 18336 扩展评估的评估者任务

评估者实施一个包含 GB/T 18336 之外要求的 PP 评估时，应当使用表 4.2 列出的 APE 类的要求。

4.3 安全目标准则概述

4.3.1 安全目标评估

ST 评估的目的是为了论证 ST 是完备的、一致的、在技术上是合理的，因此适合作为相应 TOE 评估的基础。

表 4.2 保护轮廓子类—GB/T 18336 扩展的要求

类	子类	缩写
APE 类:保护轮廓评估	保护轮廓,TOE 描述	APE _ DES
	保护轮廓,安全环境	APE _ ENV
	保护轮廓,PP 引言	APE _ INT
	保护轮廓,安全目的	APE _ OBJ
	保护轮廓,IT 安全要求	APE _ REQ
	保护轮廓,明确陈述的 IT 安全要求	**APE _ SRE**

4.3.2 与本标准其他评估准则的关系

评估 TOE 有两个明确的阶段:ST 评估和相应的 TOE 评估。在本章和第 7 章将讨论 ST 评估的要求,在第 8 章至第 15 章将讨论 TOE 评估的要求。

ST 评估包括对 PP 声明的评估。如果 ST 没有声明与 PP 的一致性,ST 的 PP 声明部分将包括这样一个陈述:TOE 没有声明与任何 PP 的一致性。

4.3.3 评估者任务

4.3.3.1 仅仅基于 GB/T 18336 要求评估的评估者任务

评估者实施一个包含在 GB/T 18336 要求之内的 ST 评估时,应当使用表 4.3 列出的 ASE 类的要求。

表 4.3 安全目标子类—仅用 GB/T 18336 的要求

类	子类	缩写
ASE 类:安全目标评估	安全目标,TOE 描述	ASE _ DES
	安全目标,安全环境	ASE _ ENV
	安全目标,ST 引言	ASE _ INT
	安全目标,安全目的	ASE _ OBJ
	安全目标,PP 声明	ASE _ PPC
	安全目标,IT 安全要求	ASE _ REQ
	安全目标,TOE 概要规范	ASE _ TSS

4.3.3.2 GB/T 18336 扩展评估的评估者任务

评估者实施一个包含 GB/T 18336 要求之外的 ST 评估时,应当使用表 4.4 列出的 ASE 类的要求。

表 4.4 安全目标子类—GB/T 18336 扩展的要求

类	子类	缩写
ASE 类:安全目标评估	安全目标,TOE 描述	ASE _ DES
	安全目标,安全环境	ASE _ ENV
	安全目标,ST 引言	ASE _ INT
	安全目标,安全目的	ASE _ OBJ
	安全目标,PP 声明	ASE _ PPC
	安全目标,IT 安全要求	ASE _ REQ
	安全目标,明确陈述的 IT 安全要求	ASE _ SRE
	安全目标,TOE 概要规范	ASE _ TSS

5 APE 类:保护轮廓评估

PP 评估的目的是论证 PP 是完备的、一致的、技术上合理的,因此评估过的 PP 适合作为 ST 开发的基础。这样的 PP 符合注册的条件。

图 5.1 给出了这个类中的子类。

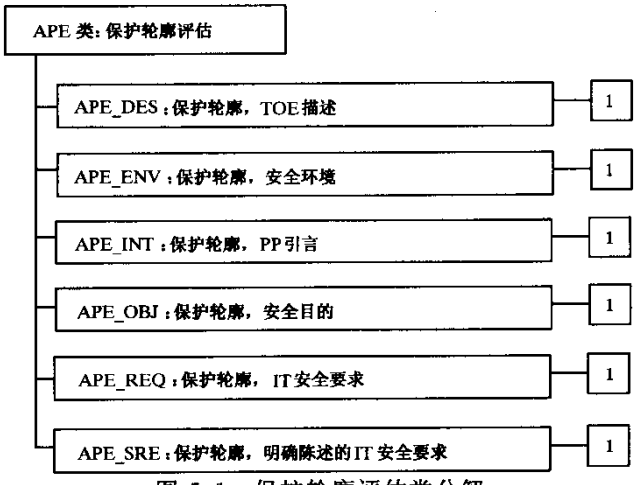

图 5.1 保护轮廓评估类分解

5.1 TOE 描述(APE _ DES)

目的:

TOE 描述有助于理解 TOE 安全要求。对 TOE 描述的评估需要说明它是连贯的、内在一致的并且与 PP 的其他部分是一致的。

APE _ DES.1 保护轮廓,TOE 描述,评估要求

依赖关系:

APE _ ENV.1 保护轮廓,安全环境,评估要求

APE _ INT.1 保护轮廓,PP 引言,评估要求

APE _ OBJ.1 保护轮廓,安全目的,评估要求

APE _ REQ.1 保护轮廓,IT 安全要求,评估要求

开发者行为元素:

APE _ DES.1.1D PP 的开发者应提供一份 TOE 描述以作为 PP 的一部分。

证据的内容和形式元素:

APE _ DES.1.1C TOE 描述应当尽量少地描述产品类型和 TOE 的一般 IT 特性。

评估者行为元素:

APE _ DES.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

APE _ DES.1.2E 评估者应确认 TOE 描述是连贯的,是内在一致的。

APE _ DES.1.3E 评估者应确认 TOE 描述与 PP 的其他部分是一致的。

5.2 安全环境(APE _ ENV)

目的:

为了确定 PP 中的 IT 安全要求是否充分,对所有评估者而言,清楚明白地理解所要解决的安全问题是很重要的。

APE _ ENV.1　保护轮廓,安全环境,评估要求

依赖关系:

无依赖关系。

开发者行为元素:

APE _ ENV.1.1D　PP 开发者应提供一份 TOE 安全环境的描述以作为 PP 的一部分。

证据的内容和形式元素:

APE _ ENV.1.1C　TOE 安全环境的陈述应当标识并且解释关于 TOE 预期用法和 TOE 使用环境的任何假设。

APE _ ENV.1.2C　TOE 安全环境的陈述应当标识并且解释任何已知的或假定的对 TOE 及其环境保护的资产的威胁。

ASE _ ENV.1.3C　TOE 安全环境的陈述应当标识并解释 TOE 必须遵守的所有组织安全策略。

评估者行为元素:

APE _ ENV.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

APE _ DES.1.2E　评估者应确认 TOE 安全环境的陈述是连贯的,是内在一致的。

5.3　PP 引言(APE _ INT)

目的:

PP 引言包括文档管理和注册一个 PP 所必需的综合信息。对 PP 引言的评估需要论证 PP 是已经正确标识的,并且它与 PP 的其他所有部分是一致的。

APE _ INT.1　保护轮廓,PP 引言,评估要求

依赖关系:

APE _ DES.1　保护轮廓,TOE 描述,评估要求

APE _ ENV.1　保护轮廓,安全环境,评估要求

APE _ OBJ.1　保护轮廓,安全目的,评估要求

APE _ REQ.1　保护轮廓,IT 安全要求,评估要求

开发者行为元素:

APE _ INT.1.1D　**PP 开发者应提供一份 PP 引言以作为 PP 的一部分。**

证据的内容和形式元素:

APE _ INT.1.1C　**PP 引言应包含一个 PP 标志,该标志提供标识、分类、登记和交叉引用这个 PP 所需要的标志性和描述性信息。**

APE _ INT.1.2C　**PP 引言应包含一个 PP 概述,以叙述的形式来概括该 PP。**

评估者行为元素:

APE _ INT.1.1E　**评估者应确认所提供的信息满足证据的内容和形式的所有要求。**

APE _ INT.1.2E　**评估者应确认 PP 引言是连贯的并且内在一致的。**

APE _ INT.1.3E　**评估者应确认 PP 引言与 PP 的其他部分是一致的。**

5.4　安全目的(APE _ OBJ)

目的:

安全目的是对安全问题意向性反应的一段简明陈述。对安全目的的评估需要论证所述的目的足以表述安全问题。安全目的分为 TOE 安全目的和环境安全目的,两者必须能追溯至已标识、可对抗的威胁或各自所需满足的策略和假设。

APE _ OBJ.1　保护轮廓,安全目的,评估要求

依赖关系:

APE _ ENV.1 **保护轮廓，安全环境，评估要求**

开发者行为元素：

APE _ OBJ.1.1D **PP 开发者应提供一份安全目的的陈述以作为 PP 的一部分。**

APE _ OBJ.1.2D **PP 开发者应提供安全目的的基本原理。**

证据的内容和形式元素：

APE _ OBJ.1.1C **安全目的的陈述应当为 TOE 及其环境定义安全目的。**

APE _ OBJ.1.2C **TOE 的安全目的应当能清楚地陈述，并且可以追溯至已标识的威胁的各个方面，这些威胁由 TOE 来对抗，同时也可以追溯至 TOE 所满足的组织安全策略。**

APE _ OBJ.1.3C **环境的安全目的应当清楚地陈述，并且可以追溯至已标识的威胁的各方面，这些威胁并非由 TOE 完全对抗，同时也可以追溯至 TOE 未完全满足的组织安全策略和假设。**

APE _ OBJ.1.4C **安全目的基本原理应当论证所陈述的安全目的适合于对抗已标识的对安全性的威胁。**

APE _ OBJ.1.5C **安全目的基本原理应当论证所述的安全目的适合于覆盖所有已标识的组织安全策略和假设。**

评估者行为元素：

APE _ OBJ.1.1E **评估者应确认所提供的信息满足证据的内容和形式的所有要求。**

APE _ OBJ.1.2E **评估者应确认安全目的的陈述是完备的、连贯的，是内在一致的。**

5.5 IT 安全要求(APE _ REQ)

目的：

有必要对一个 TOE 所选择的 IT 安全要求以及在 PP 中提出或引用的安全要求进行评估，目的是确认它们是内在一致的，并且使得该 TOE 的开发符合其安全目的。

一致的 TOE 并不需要满足对应的 PP 所描述的所有安全目的，因为有些 TOE 可能依赖于一些特定的 IT 安全要求，而这些要求是由 IT 环境所满足的。这种情况下，必须清楚地依据 TOE 要求阐述和评估环境的 IT 安全要求。

本子类提出了这样一个评估要求：它允许评估者判断一个 PP 是否适合作为一个可评估 TOE 的要求陈述。在对明确陈述的要求进行评估时，必要的附加准则包含在 APE _ SRE 子类中。

应用注释：

术语“IT 安全要求”指的是“TOE 安全要求”，有时还包括“IT 环境的安全要求”。

术语“TOE 安全要求”指的是“TOE 安全功能要求”或“TOE 安全保证要求”。

在 APE _ REQ.1 组件中，“适当的”一词用来表明在一定情况下特定的元素具有可选项。哪个选项可用，取决于在 PP 中给定的上下文环境。关于这方面的具体信息在 GB/T 18336 第 1 部分的附录 B 中有相应解释。

APE _ REQ.1 保护轮廓，IT 安全要求，评估要求

依赖关系：

APE _ OBJ.1 **保护轮廓，安全目的，评估要求**

开发者行为元素：

APE _ REQ.1.1D **PP 开发者应当提供一份 IT 安全要求的陈述以作为 PP 的一部分。**

APE _ REQ.1.2D **PP 开发者应当提供安全要求的基本原理。**

证据的内容和形式元素：

APE _ REQ.1.1C **TOE 安全功能要求的陈述应当标识从 GB/T 18336 第 2 部分功能要求组件中引用**

的 TOE 安全功能要求。

APE _ REQ.1.2C TOE 安全保证要求的陈述应当标识从本标准保证要求组件中引用的 TOE 安全保证要求。

APE _ REQ.1.3C TOE 安全保证要求的陈述应当包括一个在本标准中定义的评估保证级(EAL)。

APE _ REQ.1.4C 证据应当证明 TOE 安全保证要求的陈述是适当的。

APE _ REQ.1.5C 如果适当的话,PP 应当标识 IT 环境的所有安全要求。

APE _ REQ.1.6C 在 PP 中应当标识所有 IT 安全要求的已完成的操作。

APE _ REQ.1.7C 在 PP 中应当标识所有 IT 安全要求的未完成的操作。

APE _ REQ.1.8C 必须满足 PP 中 IT 安全要求之间的依赖关系。

APE _ REQ.1.9C 证据应当证明为何一个未满足的依赖关系却是适当的。

APE _ REQ.1.10C PP 应当包含一个关于 TOE 安全功能要求的最小功能强度级的陈述,可适当选取基本级功能强度、中级功能强度或高级功能强度中的一个。

APE _ REQ.1.11C 如果一个明确的功能强度是适当的,PP 应当标识任何特定的 TOE 安全功能要求和特定的量度。

APE _ REQ.1.12C 安全要求基本原理应当论证,PP 的最小功能强度和任何明确的功能强度声明,都是同 TOE 的安全目的一致的。

APE _ REQ.1.13C 安全要求基本原理应当论证 IT 安全要求可以满足安全目的。

APE _ REQ.1.14C 安全要求基本原理应当论证 IT 的安全要求集组成了相互支持并内在一致的一个整体。

评估者行为元素:

APE _ REQ.1.1E 评估者应当确认所提供的信息符合证据的内容和形式的所有要求。

APE _ REQ.1.2E 评估者应当确认 IT 安全要求的陈述是完备的、连贯的,是内在一致的。

5.6 明确陈述的 IT 安全要求(APE _ SRE)

目的:

经过仔细考虑,如果觉得 GB/T 18336 第 2 部分和本标准中没有一个要求组件适用于所有或部分的 IT 安全要求,PP 的作者可以陈述其他没有引用 GB/T 18336 的要求。应证明使用这种要求是适当的。

本子类提出这样一个评估要求,它允许评估者决定,明确陈述的要求的表达是否清晰且没有歧义。APE _ REQ 子类描述了对从 GB/T 18336 中引用的要求的评估和对有效且明确陈述的安全要求的评估。

需要评估明确陈述的 TOE 的 IT 安全要求,该要求是在一个 PP 中出现或被引用的,以证明其表述是清楚的,而且无歧义的。

应用注释:

形式化表示明确陈述的要求,其结构与已有的 GB/T 18336 组件和元素的结构类似,这意味着选择相似的标识方法、表示方式和详细程度。

用 GB/T 18336 要求作为一个模型,意味着这些要求可以被明确地标识,它们是自包含的,每一个要求的应用都是切实可行的,且可为该特殊要求产生 TOE 遵从声明的有意义的评估结果。

术语“IT 安全要求”指的是“TOE 安全要求”,有时还包括“IT 环境的安全要求”。

术语“TOE 安全要求”指的是“TOE 安全功能要求”或“TOE 安全保证要求”。

APE _ SRE.1 保护轮廓,明确陈述的 IT 安全要求,评估要求

依赖关系:

APE _ REQ.1　保护轮廓，IT 安全要求，评估要求

开发者行为元素：

APE _ SRE.1.1D　**PP 开发者应当提供一份 IT 安全要求的陈述以作为 PP 的一部分。**

APE _ SRE.1.2D　**PP 开发者应当提供安全要求的基本原理**

证据的内容和形式元素：

APE _ SRE.1.1C　**应当标识所有不引用 GB/T 18336 的明确陈述的 TOE 安全要求。**

APE _ SRE.1.2C　**应当标识所有不引用 GB/T 18336 的明确陈述的对 IT 环境的安全要求。**

APE _ SRE.1.3C　**证据应当证明为何这些安全要求必须被明确陈述。**

APE _ SRE.1.4C　**明确陈述的 IT 安全要求应当以 GB/T 18336 的要求组件、子类和类作为表示模型。**

APE _ SRE.1.5C　**明确陈述的 IT 安全要求应当是可度量的，并且应陈述安全目的的评估要求，这样就可以决定而且系统地论证一个 TOE 是否遵从这些要求。**

APE _ SRE.1.6C　**明确陈述的 IT 安全要求，其表达应当清楚而且无歧义。**

APE _ SRE.1.7C　**安全要求基本原理应当论证保证要求是可行的，而且适合于任何明确陈述的 TOE 安全功能要求。**

评估者行为元素：

APE _ SRE.1.1E　**评估者应当确认所提供的信息满足证据的内容和形式的所有要求。**

APE _ SRE.1.2E　评估者应当决定所有明确陈述的 IT 安全要求的依赖关系都被标识了。

6　ASE 类：安全目标评估

ST 评估的目的是论证 ST 是完备的、一致的、在技术上合理的，因而适合作为相应的 TOE 评估的基础。

图 6.1 给出这个类中的子类。

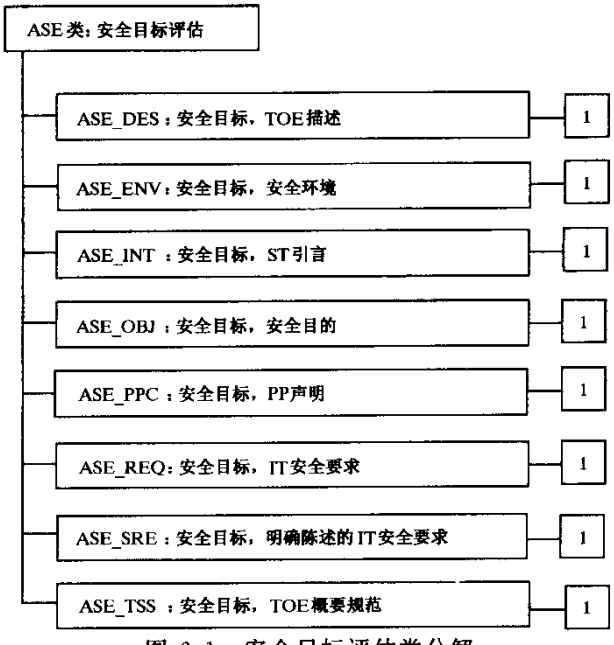

图 6.1　安全目标评估类分解

6.1　TOE 描述(ASE _ DES)

目的：

TOE 的描述有助于理解 TOE 的安全要求。对 TOE 描述的评估，需要能够表明它是连贯的、内在一

致的并且与 ST 的其他部分是一致的。

ASE _ DES.1 安全目标,TOE 描述,评估要求

依赖关系:

ASE _ ENV.1 安全目标,安全环境,评估要求

ASE _ INT.1 安全目标,ST 引言,评估要求

ASE _ OBJ.1 安全目标,安全目的,评估要求

ASE _ PPC.1 安全目标,PP 声明,评估要求

ASE _ REQ.1 安全目标,IT 安全要求,评估要求

ASE _ TSS.1 安全目标,TOE 概要规范,评估要求

开发者行为元素:

ASE _ DES.1.1D 开发者需要提供一份 TOE 的描述以作为 ST 的一部分。

证据的内容和形式元素:

ASE _ DES.1.1C TOE 描述应当尽可能少地描述产品或系统的类型、TOE 的范围和边界,在通常意义下既要用物理的方式又要用逻辑的方式来表述。

评估者行为元素:

ASE _ DES.1.1E 评估者应当确认所提供的信息都满足证据的内容和形式的所有要求。

ASE _ DES.1.2E 评估者应当确认 TOE 描述是连贯的,是内在一致的。

ASE _ DES.1.3E 评估者应当确认 TOE 的描述与 ST 其他部分是一致的。

6.2 安全环境(ASE _ ENV)

目的:

为了确定 ST 中的 IT 安全要求是否充分,有必要让所有评估者清楚地理解所要解决的安全问题。

ASE _ ENV.1 安全目标,安全环境,评估要求

依赖关系:

无依赖关系。

开发者行为元素:

ASE _ ENV.1.1D 开发者应当提供一份 TOE 安全环境的陈述以作为 ST 的一部分。

证据的内容和形式元素:

ASE _ ENV.1.1C TOE 安全环境的陈述应当标识并解释关于 TOE 的预期用法和 TOE 使用环境的任何假设。

ASE _ ENV.1.2C TOE 安全环境的陈述应当标识并解释任何已知的或假定的对 TOE 及其环境保护的资产的威胁。

ASE _ ENV.1.3C TOE 安全环境的陈述应当标识并解释 TOE 必须遵守的所有组织安全策略。

评估者行为元素:

ASE _ ENV.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ASE _ ENV.1.2E 评估者应当确认 TOE 安全环境的陈述是连贯的,并且是内在一致的。

6.3 ST 引言(ASE _ INT)

目的:

ST 引言包括标识和引用材料。对 ST 引言的评估需要论证 ST 是被正确标识的,并且与 ST 的其他部分是相一致的。

ASE _ INT.1 安全目标,ST 引言,评估要求

依赖关系：

ASE _ DES.1 安全目标，TOE 描述，评估要求

ASE _ ENV.1 安全目标，安全环境，评估要求

ASE _ OBJ.1 安全目标，安全目的，评估要求

ASE _ PPC.1 安全目标，PP 声明，评估要求

ASE _ REQ.1 安全目标，IT 安全要求，评估要求

ASE _ TSS.1 安全目标，TOE 概要规范，评估要求

开发者行为元素：

ASE _ INT.1.1D 开发者应当提供一份 ST 引言以作为 ST 的一部分。

证据的内容和形式元素：

ASE _ INT.1.1C ST 引言应当包含一个 ST 标识，它提供一些标志性和描述性的信息，而这些信息对控制和标识它所对应的 TOE 是必要的。

ASE _ INT.1.2C ST 引言应当包含一个 ST 概述，它以叙述的形式来概括该 ST。

ASE _ INT.1.3C ST 引言应当包含一个 GB/T 18336 一致性的声明，该声明陈述有关此 TOE 的任何可评估的 GB/T 18336 一致性。

评估者行为元素：

ASE _ INT.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ASE _ INT.1.2E 评估者应当确认 ST 引言是连贯的，并且是内在一致的。

ASE _ INT.1.3E 评估者应当确认 ST 引言和 ST 其他部分是一致的。

6.4 安全目的(ASE _ OBJ)

目的：

安全目的是对安全问题的意向性反应的一段简明描述。安全目标的评估需要论证，所陈述的目的足以表述安全问题。安全目的分为 TOE 的安全目的和环境的安全目的。两者必须能追溯至已标识、可对抗的威胁或各自所需满足的策略和假设。

ASE _ OBJ.1 安全目标，安全目的，评估要求

依赖关系：

ASE _ ENV.1 安全目标，安全环境，评估要求

开发者行为元素：

ASE _ OBJ.1.1D 开发者应当提供一份安全目的的陈述以作为 ST 的一部分。

ASE _ OBJ.1.2D 开发者应当提供安全目的的基本原理。

证据的内容和形式元素：

ASE _ OBJ.1.1C 安全目的的陈述应当为 TOE 及其环境定义安全目的。

ASE _ OBJ.1.2C TOE 的安全目的应当能清楚地陈述，并且可以追溯至已标识的威胁，这些威胁是由 TOE 对抗的，同时也可以追溯至 TOE 所满足的组织安全策略。

ASE _ OBJ.1.3C 环境的安全目的应当清楚地陈述，并且可以追溯至已标识的威胁的各方面，这些威胁并非由 TOE 完全对抗的，同时也可以追溯至 TOE 未完全满足的组织安全策略和假设。

ASE _ OBJ.1.4C 安全目的基本原理应当论证所陈述的安全目的适合于对抗已标识的对安全性的威胁。

ASE _ OBJ.1.5C 安全目的基本原理应当论证所陈述的安全目的适合于覆盖所有已标识的组织安全策略和假设。

评估者行为元素：

ASE _ OBJ.1.1E **评估者应当确认所提供的信息满足证据的内容和形式的所有要求。**

ASE _ OBJ.1.2E **评估者应当确认安全目的的陈述是完备的、连贯的，并且是内在一致的。**

6.5 PP 声明(ASE _ PPC)

目的：

对安全目标的 PP 声明进行评估，其目的是确定安全目标(ST)是否是 PP 的一个正确的实例化。

应用注释：

这个子类只在 ST 中有 PP 声明时适用。在其他情况下，都不需要开发者和评估者的行为。

虽然在进行 PP 声明时额外的评估是必要的，但通常对 ST 评估所花费的努力比不用 PP 时要小，因为 ST 评估可能重复使用 PP 评估的结果。

ASE _ PPC.1 安全目标，PP 声明，评估要求

依赖关系：

ASE _ OBJ.1 **安全目标，安全目的，评估要求**

ASE _ REQ.1 **安全目标，IT 安全要求，评估要求**

开发者行为元素：

ASE _ PPC.1.1D **开发者应当提供任何 PP 声明以作为 ST 的一部分。**

ASE _ PPC.1.2D **开发者应当为每一个 PP 声明提供 PP 声明的基本原理。**

证据的内容和形式元素：

ASE _ PPC.1.1C **每一个 PP 声明应当标识作了一致性声明的 PP，包括该声明所需要的限制。**

ASE _ PPC.1.2C **每一个 PP 声明应当标识那些符合 PP 的许可操作的 IT 安全要求陈述或者进一步限制 PP 的要求。**

ASE _ PPC.1.3C **每一个 PP 声明应当标识那些包含在 ST 中的安全目的和 IT 安全要求陈述，它们在 PP 中是作为附加信息出现的。**

评估者行为元素：

ASE _ PPC.1.1E **评估者应当确认所提供的信息满足证据的内容和形式的所有要求。**

ASE _ PPC.1.2E **评估者应当确认 PP 声明是 PP 的一个正确实例化。**

6.6 IT 安全要求(ASE _ REQ)

目的：

有必要对一个 TOE 所选择的的 IT 安全要求以及在 PP 中提出或引用的安全要求进行评估，目的是确认它们是内在一致的，并且使得该 TOE 的开发符合其安全目的。本子类提出了这样一个评估要求：它允许评估者决定一个 ST 是否适合作为一个相应 TOE 的要求陈述。在对明确陈述的要求进行评估时，必要的附加准则应包含在 ASE _ SRE 子类中。

应用注释：

术语“IT 安全要求”指的是“TOE 安全要求”，有时也包含“IT 环境的安全要求”。

术语“TOE 安全要求”指的是“TOE 安全功能要求”或“TOE 安全保证要求”。

在 ASE _ REQ.1 组件中，“适当的”一词用来表明在一定情况下特定的元素具有可选项。哪个选项可用，取决于在 ST 中给定的上下文环境。关于这方面的具体信息在 GB/T 18336 第 1 部分的附录 C 中有相应解释。

ASE _ REQ.1 安全目标，IT 安全要求，评估要求

依赖关系：

ASE _ OBJ.1 安全目标，安全目的，评估要求

开发者行为元素：

ASE _ REQ.1.1D 开发者应当提供一份 IT 安全要求的陈述以作为 ST 的一部分。

ASE _ REQ.1.2D 开发者应当提供安全要求的基本原理。

证据的内容和形式元素：

ASE _ REQ.1.1C TOE 安全功能要求的陈述应当标识从 GB/T 18336 第 2 部分功能要求组件中引用的 TOE 安全功能要求。

ASE _ REQ.1.2C TOE 安全保证要求的陈述应当标识从本标准保证要求组件中引用的 TOE 安全保证要求。

ASE _ REQ.1.3C TOE 安全保证要求的陈述应当包含一个在本标准定义的评估保证级(EAL)。

ASE _ REQ.1.4C 证据应当证明 TOE 安全保证要求的陈述是恰当的。

ASE _ REQ.1.5C 如果适当的话，ST 应当标识 IT 环境的任何安全要求。

ASE _ REQ.1.6C 应当指明并完成所有包含在 ST 中的 IT 安全要求的操作。

ASE _ REQ.1.7C 必须满足 ST 中 IT 安全要求之间的依赖关系。

ASE _ REQ.1.8C 证据应当证明为何一个未满足的依赖关系却是适当的。

ASE _ REQ.1.9C ST 应当包含一个关于 TOE 安全功能要求的最小功能强度级的陈述，可适当选取基本级功能强度、中级功能强度或高级功能强度中的一个。

ASE _ REQ.1.10C ST 应当指明任何特定的 TOE 安全功能要求对一个明确的功能强度和特定的尺度是适当的。

ASE _ REQ.1.11C 安全要求基本原理应当论证，ST 的最小功能强度和任何明确的功能强度声明，都是同 TOE 的安全目的一致的。

ASE _ REQ.1.12C 安全要求基本原理应当论证 IT 安全要求可以满足安全目的。

ASE _ REQ.1.13C 安全要求基本原理应当论证 IT 的安全要求集组成了相互支持和内在一致的一个整体。

评估者行为元素：

ASE _ REQ.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ASE _ REQ.1.2E 评估者应当确认 IT 安全要求陈述是完备的、连贯的，并且是内在一致的。

6.7 明确陈述的 IT 安全要求(ASE _ SRE)

目的：

经过仔细考虑，如果觉得 GB/T 18336 第 2 部分和本标准中没有一个要求组件适用于所有或部分的 IT 安全要求，ST 的作者可以陈述其他不需要引用 GB/T 18336 的要求。使用这种要求将被证明是适当的。

本子类提出这样一个评估要求，它允许评估者决定，明确陈述的要求的表达是否清晰且没有歧义。ASE _ REQ 子类描述了对从 GB/T 18336 中引用的要求的评估和对有效且明确陈述的安全要求的评估。

需要评估明确陈述的 TOE 的 IT 安全要求，该要求是在一个 ST 中出现或被引用的，以证明其表述是清楚的，而且无歧义的。

应用注释：

形式化表示明确陈述的要求，其结构与已有的 GB/T 18336 组件和元素的结构类似，这意味着选择相似的标识方法、表示方式和详细程度。

用 GB/T 18336 要求作为一个模型，意味着这些要求可以被明确地标识，它们是自包含的，每一个要求的应用都是切实可行的，且可为该特殊要求产生 TOE 遵从声明的有意义的评估结果。

术语“IT 安全要求”指的是“TOE 安全要求”，有时还包括“IT 环境的安全要求”。

术语“TOE 安全要求”指的是“TOE 安全功能要求”或“TOE 安全保证要求”。

ASE _ SRE.1 安全目标，明确陈述的 IT 安全要求，评估要求

依赖关系：

ASE _ REQ.1 **安全目标，IT 安全要求，评估要求**

开发者行为元素：

ASE _ SRE.1.1D **开发者应当提供一份 IT 安全要求的陈述以作为 ST 的一部分。**

ASE _ SRE.1.2D **开发者应当提供安全要求的基本原理。**

证据的内容和形式元素：

ASE _ SRE.1.1C **应当指明所有不引用 GB/T 18336 的明确陈述的 TOE 安全要求。**

ASE _ SRE.1.2C **应当指明所有不引用 GB/T 18336 的明确陈述的对 IT 环境的安全要求。**

ASE _ SRE.1.3C **证据应当证明为何这些安全要求必须被明确陈述。**

ASE _ SRE.1.4C **明确陈述的 IT 安全要求应当以 GB/T 18336 的要求组件、子类和类作为表示模型。**

ASE _ SRE.1.5C **明确陈述的 IT 安全要求应当是可度量的，并且应陈述安全目的的评估要求，这样就可以判断而且系统地论证一个 TOE 是否遵照这些要求。**

ASE _ SRE.1.6C **明确陈述的 IT 安全要求，其表达应当清楚而且无歧义。**

ASE _ SRE.1.7C **安全要求基本原理应当论证保证要求是可行的，而且适合于任何明确陈述的 TOE 安全功能要求。**

评估者行为元素：

ASE _ SRE.1.1E **评估者应当确认所提供的信息满足证据的内容和形式的所有要求。**

ASE _ SRE.1.2E **评估者应当决定所有明确陈述的 IT 安全要求的依赖关系都被标识了。**

6.8 TOE 概要规范（ASE _ TSS）

目的：

TOE 概要规范，在高层定义了声称满足功能要求的安全功能以及为满足保证要求而采取的保证措施。

应用注释：

IT 安全功能和 TOE 安全功能要求之间的关系是一种“多对多”的关系。然而，为了能够清楚地定义 TSF，每一个安全功能应有助于满足至少一个安全要求。不能实现这种要求的安全功能通常是不需要的。注意，安全功能有助于满足至少一个安全要求，这个要求是用非常一般的方式来表达的，因此对 TOE 而言应当证明所有的安全功能都是有用的。

ST 中包含了不是从 GB/T 18336 中引用的保证要求时，保证措施的陈述是尤其适用的。如果 ST 中的 TOE 安全保证要求都只基于 GB/T 18336 评估保证级或其他 GB/T 18336 保证组件，那么保证措施可以通过引用有关文献来提出，这些文献表明这些保证要求已经得到了满足。

在 ASE _ TSS.1 组件中，“适当的”一词用来表明在一定情况下特定的元素具有可选项。哪个选项可用，取决于在 ST 中给定的上下文环境。关于这方面的具体信息在 GB/T 18336 第 1 部分的附录 C 中有相应解释。

ASE _ TSS.1 安全目标，TOE 概要规范，评估要求

依赖关系：

ASE _ REQ.1 **安全目标，IT 安全要求，评估要求**

开发者行为元素：

ASE_TSS.1.1D **开发者应当提供一份 TOE 概要规范以作为 ST 的一部分。**

ASE_TSS.1.2D **开发者应当提供 TOE 概要规范的基本原理。**

证据的内容和形式元素：

ASE_TSS.1.1C **TOE 概要规范应当描述 TOE 的 IT 安全功能和保证措施。**

ASE_TSS.1.2C **TOE 概要规范应当从 IT 安全功能追溯到 TOE 安全功能要求，这样就能看出哪个 IT 安全功能满足了哪个 TOE 安全功能要求，也能看出每个 IT 安全功能有助于满足至少一个 TOE 安全功能要求。**

ASE_TSS.1.3C **应当用一个非形式化的方式定义 IT 安全功能，其详细程度应达到可以理解这些功能的目的。**

ASE_TSS.1.4C **对 ST 中所有安全机制的引用，应当追溯其相应的安全功能，这样就能看出在实现每个功能时相应地使用了哪些安全机制。**

ASE_TSS.1.5C **TOE 概要规范的基本原理应当论证 IT 安全功能足以满足 TOE 安全功能要求。**

ASE_TSS.1.6C **TOE 概要规范的基本原理应当论证，特定的 IT 安全功能组合在一起能够满足 TOE 安全功能要求。**

ASE_TSS.1.7C **TOE 概要规范应当从保证措施追溯到其保证要求，这样就能看出哪个措施有助于满足哪个要求。**

ASE_TSS.1.8C **TOE 概要规范的基本原理应当论证保证措施满足 TOE 所有的保证要求。**

ASE_TSS.1.9C **TOE 概要规范应当指明所有采用概率或排列机制实现的 IT 安全功能是适当的。**

ASE_TSS.1.10C **TOE 概要规范应当为每一个适当的 IT 安全功能陈述其功能强度声明，或者用一个特定的尺度，或者用基本级功能强度、中级功能强度、高级功能强度中的一个。**

评估者行为元素：

ASE_TSS.1.1E **评估者应当确认所提供的信息满足证据的内容和形式的所有要求。**

ASE_TSS.1.2E **评估者应当确认 TOE 概要规范是完备的、连贯的，并且是内在一致的。**

7 评估保证级

评估保证级(EAL)提供了一个递增的尺度，该尺度的确定权衡了所获得的保证级与以及达到该保证程度所需的代价和可行性。GB/T 18336 方法确定了在评估结束时 TOE 中保证的几个不同概念，以及在 TOE 运行使用过程中对保证进行维护的几个不同概念。

并非本标准中的所有子类和组件都包括在这些 EAL 中，这一点是很值得注意的。这并不是说没有包含在 EAL 中的这些子类和组件不提供有意义的和所需要的保证。相反，我们希望能把这些子类和组件当作是为使 PP 和 ST 更实用，而对其中的一个 EAL 的增强。

7.1 评估保证级(EAL)概述

表 7.1 概括性地描述了几个 EAL。其中列表示的是一组按级排序的 EAL，行表示的是保证子类。在结果矩阵中的每一个数字都标识了此处适宜的一个具体保证组件。

正如在 7.2 条里所总结的那样，在 GB/T 18336 中对 TOE 的保证等级定义了七个按级排序的的评估保证级。它们按级别排序，因为每一个 EAL 要比所有较低的 EAL 表达更多的保证。从 EAL 到 EAL 的保证的不断增加，靠替换成同一保证子类中的一个更高级别的保证组件（即增加严格性、范围或深度）和添加另外一个保证子类的保证组件(例如，添加新的要求）得以实现。

正如在本标准第 3 章阐述的那样，这些 EAL 由保证组件的一个适当组合组成。更确切地说，每个 EAL 仅仅包含每个保证子类的一个组件，以及罗列了每个组件的所有保证依赖关系。

虽然这些 EAL 是在 GB/T 18336 中定义的，但还是可以用来表示保证的其他组合。特别地，“增强”这个概念允许(从没有包括在 EAL 中的保证子类)向 EAL 中增加保证组件，或允许对一个 EAL（用同一个保证子类的其他更高级别的保证组件）替换保证组件。在 GB/T 18336 中定义的保证结构中，只有

EAL 可以增强。“EAL 减去一个组成保证组件”这一概念在本标准中不认为是一个有效的声明。在声明的部分，“增强”有义务证明其实用性以及对 EAL 添加保证组件的额外价值。一个 EAL 也可以用明确陈述的保证要求来扩充。

表 7.1　评估保证级汇总

保证类	保证子类		评估保证级(EAL)依据的保证组件						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
配置管理	ACM _ AUT	CM 自动化				1	1	2	2
	ACM _ CAP	CM 能力	1	2	3	4	4	5	5
	ACM _ SCP	CM 范围			1	2	3	3	3
交付和运行	ADO _ DEL	交付		1	1	2	2	2	3
	ADO _ IGS	安装、生成和启动	1	1	1	1	1	1	1
开发	ADV _ FSP	功能规范	1	1	1	2	3	3	4
	ADV _ HLD	高层设计		1	2	2	3	4	5
	ADV _ IMP	实现表示				1	2	3	3
	ADV _ INT	TSF 内部					1	2	3
	ADV _ LLD	低层设计				1	1	2	3
	ADV _ RCR	表示对应性	1	1	1	1	2	2	3
	ADV _ SPM	安全策略模型				1	3	3	3
指导性文档	AGD _ ADM	管理员指南	1	1	1	1	1	1	1
	AGD _ USR	用户指南	1	1	1	1	1	1	1
生命周期支持	ALC _ DVS	开发安全			1	1	1	2	2
	ALC _ FLR	缺陷纠正							
	ALC _ LCD	生命周期定义				1	2	2	3
	ALC _ TAT	工具和技术				1	2	3	3
测试	ATE _ COV	覆盖范围		1	2	2	2	3	3
	ATE _ DPT	深度			1	1	2	2	3
	ATE _ FUN	功能测试		1	1	1	1	2	2
	ATE _ IND	独立性测试	1	2	2	2	2	2	3
脆弱性评定	AVA _ CCA	隐蔽信道分析					1	2	2
	AVA _ MSU	误用			1	2	2	3	3
	AVA _ SOF	TOE 安全功能强度		1	1	1	1	1	1
	AVA _ VLA	脆弱性分析		1	1	2	3	4	4

7.2　评估保证级细节

以下 7.2.1～7.2.7 提供这些 EAL 的定义，用粗体字突出表示特定的要求与这些要求的散文化特征描述的区别。

7.2.1　评估保证级 1(EAL1)——功能测试

目的：

EAL1 适用于在对正确运行需要一定信任的场合，但在该场合中对安全的威胁应视为并不严重。

它还适用于需要独立的保证来支持以下论点的情况，该论点认为在人员或类似信息的保护方面已经给予足够的重视。

EAL1 为用户提供了 TOE 的一个评估，包括依据一个规范的独立性测试和对所提供的指导性文档的检查。预计在没有 TOE 开发者的帮助下，一个 EAL1 评估也能成功地进行而且所需费用最少。

在这个级别上的一个评估应当提供这样的证据，即 TOE 的功能与其文档在形式上是一致的，并且对已标识的威胁提供了有效的保护。

保证组件：

EAL1(参见表 7.2)通过利用功能和接口的规范以及指导性文档，对安全功能进行分析来提供一种基础级别的保证，以理解安全行为。

这种分析由对 TOE 安全功能的独立性测试来支持。

和未经评估的 IT 产品或系统相比，本 EAL 提供了保证的有意义增长。

表 7.2 评估保证级 1

保证类	保证组件
配置管理	ACM _ CAP.1 版本号
交付和运行	ADO _ IGS.1 安装、生成和启动程序
开发	ADV _ FSP.1 非形式化功能规范
	ADV _ RCR.1 非形式化对应性论证
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
测试	ATE _ IND.1 独立性测试——一致性

7.2.2 评估保证级 2(EAL2)——结构测试

目的：

在交付设计信息和测试结果时，EAL2 需要开发者的合作，但不应超出与良好商业运作的一致性，而要求开发方付出更多的努力。这样，就不需要增加过多的费用或时间的投入。

因此 EAL2 适用于以下这种情况：在缺乏现成可用的完整的开发记录时，开发者或使用者需要一种低到中等级别的独立保证的安全性。在传统的保密系统或者同开发者的访问受到限制时，可能会出现以上这种情况。

保证组件：

EAL2(参见表 7.3)通过利用功能和接口的规范、指导性文档和 TOE 的高层设计，对安全功能进行分析来提供保证，以理解安全行为。

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，**开发者基于功能规范进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索明显的脆弱性(如，公开的脆弱性)的证据。**

EAL2 也通过 TOE 的配置表和安全交付程序的证据来提供保证。

本 EAL 在 EAL1 基础上有意义地增加了保证，这是通过要求开发者测试，以及脆弱性分析和基于更详细的 TOE 规范的独立性测试来实现的。

表 7.3 评估保证级 2

保证类	保证组件
配置管理	ACM _ CAP.2 配置项
交付和运行	ADO _ DEL.1 交付程序
	ADO _ IGS.1 安装、生成和启动程序
开发	ADV _ FSP.1 非形式化功能规范
	ADV _ HLD.1 描述性高层设计
	ADV _ RCR.1 非形式化对应性论证
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
测试	ATE _ COV.1 范围证据
	ATE _ FUN.1 功能测试
	ATE _ IND.2 独立性测试——抽样
脆弱性评定	AVA _ SOF.1 TOE 安全功能强度评估
	AVA _ VLA.1 开发者脆弱性分析

7.2.3 评估保证级 3(EAL3)——系统地测试和检查

目的：

EAL3 可使一个尽职尽责的开发者在设计阶段能从正确的安全工程中获得最大限度的保证，而不需要对现有的合理的开发实践作大规模的改变。

EAL3 适用于以下这些情况：开发者或使用者需要一个中等级别的独立保证的安全性，和在没有再次进行真正的工程实践的情况下，要求对 TOE 及其开发过程进行彻底调查。

保证组件：

EAL3(参见表 7.4)通过利用功能和接口的规范、指导性文档和 TOE 的高层设计，对安全功能进行分析来提供保证，以理解安全行为。

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，开发者基于功能规范和高层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索明显的脆弱性(如，公开的脆弱性)的证据。

EAL3 还通过使用开发环境控制措施、TOE 的配置管理和安全交付程序的证据来提供保证。

本 EAL 在 EAL2 的基础上有意义地增加了保证，这是通过要求更完备的安全功能测试范围，以及要求一些提供 TOE 在开发过程中不会被篡改的可信性的机制或程序来实现的。

表 7.4 评估保证级 3

保证类	保证组件
配置管理	ACM _ CAP.3 授权控制
	ACM _ SCP.1 TOE 配置管理(CM)范围
交付和运行	ADO _ DEL.1 交付程序
	ADO _ IGS.1 安装、生成和启动程序
开发	ADV _ FSP.1 非形式化功能规范
	ADV _ HLD.2 安全加强的高层设计
	ADV _ RCR.1 非形式化对应性论证
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南

表 7.4（完）

保证类	保证组件
生命周期支持	ALD_DVS.1 安全措施标识
测试	ATE_COV.2 范围分析
	ATE_DPT.1 测试：高层设计
	ATE_FUN.1 功能测试
	ATE_IND.2 独立性测试——抽样
脆弱性评定	AVA_MSU.1 指南审查
	AVA_SOF.1 TOE 安全功能强度评估
	AVA_VLA.1 开发者脆弱性分析

7.2.4 评估保证级 4(EAL4)——系统地设计、测试和复查

目的：

EAL4 可使开发者从正确的安全工程中获得最大限度的保证，这种安全工程基于良好的商业开发实践，这种实践虽然很严格，但并不需要大量专业知识、技巧和其他资源。在经济合理的条件下，对一个已经存在的生产线进行翻新时，EAL4 是所能达到的最高级别。

因此 EAL4 适用于以下这两种情况：开发者或使用者对传统的商品化的 TOE 需要一个中等到高等级别的独立保证的安全性，和准备负担额外的安全专用工程费用。

保证组件：

EAL4(参见表 7.5)通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层设计和低层设计、实现的子集，对安全功能进行分析来提供保证，以理解安全行为。也可通过 TOE 安全策略的一个非形式化模型来额外地获得保证。

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，开发者基于功能规范和高层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御低等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析。

EAL4 还通过使用开发环境控制措施、包括自动化在内的额外的 TOE 配置管理以及安全交付程序的证据来提供保证。

本 EAL 在 EAL3 基础上有意义地增加了保证，这是通过要求更多的设计描述、实现的子集，以及提供 TOE 在开发或交付过程中不会被篡改的可信性的改进机制或程序来实现的。

表 7.5 评估保证级 4

保证类	保证组件
配置管理	ACM_AUT.1 部分配置管理(CM)自动化
	ACM_CAP.4 产生支持和接受程序
	ACM_SCP.2 跟踪配置管理(CM)范围问题
交付和运行	ADO_DEL.2 修改检测
	ADO_IGS.1 安装、生成和启动程序
开发	ADV_FSP.2 完全定义的外部接口
	ADV_HLD.2 安全加强的高层设计
	ADV_IMP.1 TSF 实现的子集
	ADV_LLD.1 描述性低层设计
	ADV_RCR.1 非形式化对应性论证
	ADV_SPM.1 非形式化 TOE 安全策略模型

表 7.5（完）

保证类	保证组件
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
生命周期支持	ALC _ DVS.1 安全措施标识
	ALC _ LCD.1 开发者定义的生命周期模型
	ALC _ TAT.1 明确定义的开发工具
测试	ATE _ COV.2 范围分析
	ATE _ DPT.1 测试：高层设计
	ATE _ FUN.1 功能测试
	ATE _ IND.2 独立性测试——抽样
脆弱性评定	**AVA _ MSU.2 分析确认**
	AVA _ SOF.1 TOE 安全功能强度评估
	AVA _ VLA.2 独立脆弱性分析

7.2.5 评估保证级 5（EAL5）——半形式化设计和测试

目的：

EAL5 可使一个开发者从安全工程中获得最大限度的保证，这种安全工程所基于的严格的商业开发实践，是靠适度应用专业安全工程技术来支持的。设计和开发这样的 TOE 需要有达到 EAL5 保证的决心。相对于没有应用专业技术的严格开发而言，由 EAL5 要求引起的额外的开销也许不会很大。

因此 EAL5 适用于以下这些情况：开发者和使用者在有计划的开发中需要一个高级别的独立保证的安全性，和在没有由专业安全工程技术引起不合理开销的条件下，需要一种严格的开发手段。

保证组件：

EAL5（参见表 7.6）通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及**所有的**实现，对安全功能进行分析来提供保证，以理解安全行为。也可以通过以下这些方式额外地获得保证：TOE 安全策略的**形式化模型，功能规范和高层设计的半形式化表示，以及它们之间对应性的半形式化论证。此外还需要一个模块化的 TOE 设计。**

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，开发者基于功能规范、高层设计**和低层设计**进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御**中等**攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析。**这种分析也包括对开发者的隐蔽信道分析的确认。**

EAL5 还通过使用开发环境控制措施、包括自动化在内的**全面的 TOE** 配置管理以及安全交付程序的证据来提供保证。

本 EAL 在 EAL4 的基础上有意义地增加了保证，这是通过要求半形式化的设计描述、整个实现，更结构化（因而更具有可分析性）的体系，隐蔽信道分析，以及提供 TOE 在开发过程中不会被篡改的可信性的改进机制或程序来实现的。

表 7.6 评估保证级 5

保证类	保证组件
配置管理	ACM _ AUT.1 部分配置管理（CM）自动化
	ACM _ CAP.4 产生支持和接受程序
	ACM _ SCP.3 开发工具配置管理（CM）范围

表 7.6（完）

保证类	保证组件
交付和运行	ADO _ DEL.2 修改检测
	ADO _ IGS.1 安装、生成和启动过程
开发	**ADV _ FSP.3 半形式化功能规范**
	ADV _ HLD.3 半形式化高层设计
	ADV _ IMP.2 TSF 实现
	ADV _ INT.1 模块化
	ADV _ LLD.1 描述性低层设计
	ADV _ RCR.2 半形式化对应性论证
	ADV _ SPM.3 形式化 TOE 安全策略模型
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
生命周期支持	ALC _ DVS.1 安全措施标识
	ALC _ LCD.2 标准化生命周期模型
	ALC _ TAT.2 遵从实现标准
测试	ATE _ COV.2 范围分析
	ATE _ DPT.2 测试：低层设计
	ATE _ FUN.1 功能测试
	ATE _ IND.2 独立性测试——抽样
脆弱性评定	**AVA _ CCA.1 隐蔽信道分析**
	AVA _ MSU.2 分析确认
	AVA _ SOF.1 TOE 安全功能强度评估
	AVA _ VLA.3 中级抵抗力

7.2.6 评估保证级 6（EAL6）——半形式化验证的设计和测试

目的：

EAL6 可使开发者通过把安全工程技术应用于严格的开发环境，而获得高度的保证，以便生产一个昂贵的 TOE 来保护高价值的资产对抗重大的风险。

因此 EAL6 适用于以下情况：应用于高风险环境下的安全 TOE 的开发，在这里受保护的资源值得花费额外的开销。

保证组件：

EAL6（参见表 7.7）通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及实现的**结构化表示**，对安全功能进行分析来提供保证，以理解安全行为。还通过以下这些方式额外地获得保证：TOE 安全策略的形式化模型，功能规范、高层设计**和低层设计**的半形式化表示，以及它们之间对应性的半形式化论证。此外还需要一个模块化和**分层的** TOE 设计。

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，开发者基于功能规范、高层设计和低层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御**高等**攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析。这种分析也

包括对开发者的系统化隐蔽信道分析的确认。

EAL6 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

本 EAL 在 EAL5 的基础上有意义地增加了保证，这是通过要求更全面的分析、实现的结构化表示、更体系化的结构（如，分层）、更全面的独立脆弱性分析、系统化隐蔽信道识别，以及改进了的配置管理和开发环境控制等来实现的。

表 7.7 评估保证级 6

保证类	保证组件
配置管理	ACM _ AUT.2 完全配置管理(CM)自动化
	ACM _ CAP.5 高级支持
	ACM _ SCP.3 开发工具配置管理(CM)范围
交付和运行	ADO _ DEL.2 修改检测
	ADO _ IGS.1 安装、生成和启动程序
开发	ADV _ FSP.3 半形式化功能规范
	ADV _ HLD.4 半形式化高层解释
	ADV _ IMP.3 TSF 的结构化实现
	ADV _ INT.2 复杂性降低
	ADV _ LLD.2 半形式化低层设计
	ADV _ RCR.2 半形式化对应性论证
	ADV _ SPM.3 形式化 TOE 安全策略模型
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
生命周期支持	ALC _ DVS.2 安全措施的充分性
	ALC _ LCD.2 标准化生命周期模型
	ALC _ TAT.3 遵从实现标准——所有部分
测试	ATE _ COV.3 范围的严格分析
	ATE _ DPT.2 测试：低层设计
	ATE _ FUN.2 顺序的功能测试
	ATE _ IND.2 独立性测试——抽样
脆弱性评定	AVA _ CCA.2 系统化隐蔽信道分析
	AVA _ MSU.3 对非安全状态的分析和测试
	AVA _ SOF.1 TOE 安全功能强度评估
	AVA _ VLA.4 高级抵抗力

7.2.7 评估保证级 7(EAL7)——形式化验证的设计和测试

目的：

EAL7 适用于安全 TOE 的开发，该 TOE 将应用在风险非常高的地方或有高价值资产值得更高的开销的地方。EAL7 的实际应用目前只局限于一些 TOE，这些 TOE 非常关注能经受广泛地形式化分析的安全功能。

保证组件：

EAL7（参见表 7.8）通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及实现的结构化表示，对安全功能进行分析来提供保证，以理解安全行为。也可通过以下这些方式额外地获得保证：TOE 安全策略的形式化模型、**功能规范和高层设计的形式化表示**、低层设计的半形式化表示，以及它们之间对应性的**适当的形式化**和半形式化论证。此外还需要一个模块化的、分层的且**简单的** TOE 设计。

这种分析由以下诸因素来提供支持：TOE 安全功能的独立性测试，开发者基于功能规范、高层设计、低层设计和**实现表示**进行测试得到的证据，对开发者测试结果的**全部**独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御高等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析。这种分析也包括对开发者的系统化隐蔽信道分析的确认。

EAL7 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

本 EAL 在 EAL6 的基础上有意义地增加了保证，这是通过要求利用形式化表示和形式化对应性进行更全面的分析，以及更全面的测试来实现的。

表 7.8　评估保证级 7

保证类	保证组件
配置管理	ACM _ AUT.2 完全配置管理(CM)自动化
	ACM _ CAP.5 高级支持
	ACM _ SCP.3 开发工具配置管理(CM)范围
交付和运行	**ADO _ DEL.3 修改预防**
	ADO _ IGS.1 安装、生成和启动过程
开发	**ADV _ FSP.4 形式化功能规范**
	ADV _ HLD.5 形式化高层设计
	ADV _ IMP.3 TSF 的结构化实现
	ADV _ INT.3 复杂性最小化
	ADV _ LLD.2 半形式化低层设计
	ADV _ RCR.3 形式化对应性论证
	ADV _ SPM.3 形式化 TOE 安全策略模型
指导性文档	AGD _ ADM.1 管理员指南
	AGD _ USR.1 用户指南
生命周期支持	ALC _ DVS.2 安全措施的充分性
	ALC _ LCD.3 可测量的生命周期模型
	ALC _ TAT.3 遵从实现标准——所有部分
测试	ATE _ COV.3 范围的严格分析
	ATE _ DPT.3 测试：实现表示
	ATE _ FUN.2 顺序的功能测试
	ATE _ IND.3 独立性测试——全部
脆弱性评定	AVA _ CCA.2 系统化隐蔽信道分析
	AVA _ MSU.3 对非安全状态的分析和测试
	AVA _ SOF.1 TOE 安全功能强度评估
	AVA _ VLA.4 高级抵抗力

8 保证类、子类和组件

下面七章按字母顺序，以类和子类进行分组，给出了每一个保证组件的详细要求。

9 ACM 类：配置管理

配置管理(CM)是一种建立功能要求和规范的方法或方式，该功能要求和规范在 TOE 实现中具体实施。CM 通过在 TOE 和相关信息的细化和修改过程中，要求一定的秩序和控制，以达到其目的。通过提供跟踪任何变化的方法和确保所有修改都已授权，实现 CM 系统以确保它们所控制的 TOE 各部分的完整性。

图 9.1 给出了该类中包含的子类以及子类内组件的层次结构。

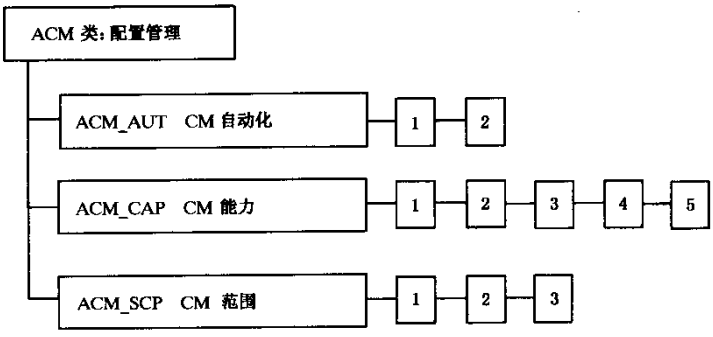

图 9.1 配置管理类分解

9.1 CM 自动化(ACM _ AUT)

目的：

介绍自动 CM 工具的目的是为了增加 CM 系统的有效性。虽然自动的 CM 系统和手工的 CM 系统都能被旁路或忽视，或者不能充分证实其可以防止未授权的修改，但是自动的系统不易受人为错误或疏忽的影响。

组件分级：

本子类组件的分级是基于自动方式所控制的配置项集合的。

应用注释：

ACM _ AUT. 1. 1C 引入一个与 TOE 实现表示相关的要求。TOE 实现表示包括组成物理 TOE 的所有硬件、软件和固件。就纯软件 TOE 而言，实现表示可能只包括源代码和目标代码。

ACM _ AUT. 1. 2C 引入一个由 CM 系统提供一种自动方式来支持 TOE 的生成的要求。要求 CM 系统提供一种自动方式以协助确定在 TOE 的生成中使用了正确的配置项。

ACM _ AUT. 2. 5C 引入一个由 CM 系统提供一种自动方式来确定 TOE 和它以前版本之间的变化的要求。如果 TOE 不存在以前版本，开发者仍需要提供一种自动方式来确定 TOE 和它将来版本之间的变化。

ACM _ AUT. 1 部分 CM 自动化

目的：

当实现表示很复杂或由多个开发者合作开发时，在这样的开发环境中不使用自动工具来控制变化是很困难的。特别地，这些自动工具还必须能够应付在开发过程中出现的多种变化，并确保这些变化都是已授权的。本组件的目的就是确保实现表示是通过自动方式控制的。

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ACM _ AUT.1.1D 开发者应该使用 CM 系统。

ACM _ AUT.1.2D 开发者应该提供 CM 计划。

证据的内容和形式元素：

ACM _ AUT.1.1C CM 系统应该提供一种自动方式，通过该方式确保只能对 TOE 的实现表示进行已授权的改变。

ACM _ AUT.1.2C CM 系统应该提供一种自动方式来支持 TOE 的生成。

ACM _ AUT.1.3C CM 计划应该描述在 CM 系统中所使用的自动工具。

ACM _ AUT.1.4C CM 计划应该描述在 CM 系统中如何使用自动工具。

评估者行为元素：

ACM _ AUT.1.1E 评估者应该确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ AUT.2 完全 CM 自动控制

目的：

当配置项很复杂或由多个开发者合作开发时，在这样的开发环境中不使用自动工具来控制变化是很困难的。特别地，这些自动工具还必须能够支持在开发过程中出现的多种变化，并确保这些变化都是已授权的。本组件的目的就是确保所有的配置项都是通过自动方式控制的。

本组件提供一种自动方式以确定 TOE 版本间的变化，并且标识哪个配置项会因其修改而影响其余配置项，这就有助于确定 TOE 后继版本间变化的影响。如此轮流进行就可得到一些非常有用的信息，以确定 TOE 改变后所有配置项是否还相互一致。

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ACM _ AUT.2.1D 开发者应该使用 CM 系统。

ACM _ AUT.2.2D 开发者应该提供 CM 计划。

证据的内容和形式元素：

ACM _ AUT.2.1C CM 系统应该提供一种自动方式，通过该方式确保只能对 TOE 的实现表示和所有其他的配置项进行已授权的改变。

ACM _ AUT.2.2C CM 系统应该提供一种自动方式来支持 TOE 的生成。

ACM _ AUT.2.3C CM 计划应该描述在 CM 系统中所使用的自动工具。

ACM _ AUT.2.4C CM 计划应该描述在 CM 系统中如何使用自动工具。

ACM _ AUT.2.5C CM 系统应该提供一种自动方式以确定 TOE 和它以前版本之间的变化。

ACM _ AUT.2.6C CM 系统应该提供一种自动方式以确定因给定的配置项的修改而受到影响的其他所有配置项。

评估者行为元素：

ACM _ AUT.2.1E 评估者应该确认所提供的信息满足证据的内容和形式的所有要求。

9.2 CM 能力(ACM _ CAP)

目的：

CM 系统的能力表明了对配置项的意外或未授权的修改发生的可能性。CM 系统从早期设计阶段到整个后继维护过程中都应该确保 TOE 的完整性。

本子类的目的包括以下方面：

a）确保 TOE 在送给用户之前是正确和完备的；

b）确保在评估过程中没有丢失任何配置项；

c）防止对 TOE 配置项进行未授权的修改、增加或删除。

组件分级：

本子类组件的分级，依据 CM 系统能力、开发者提供的 CM 文档的范围以及开发者是否证明了 CM 系统满足安全要求等因素。

应用注释：

ACM _ CAP. 2 引入了几个与配置项有关的元素。ACM _ SCP 子类包含一些由 CM 系统跟踪的有关配置项的要求。

ACM _ CAP. 2. 3C 引入了一个应提供配置清单的要求。配置清单包括所有由 CM 系统维护的配置项。

ACM _ CAP. 2. 6C 引入了一个 CM 系统应唯一标识所有配置项的要求。这也要求给修改后的配置项分配一个新的唯一标识符。

ACM _ CAP. 3. 8C 引入了一个关于证据应论证 CM 的系统运作与 CM 计划相一致的要求。这些证据的例子可以是诸如屏幕快照、CM 系统输出的审计迹或开发者提供的 CM 系统详细论证等文档。评估者有责任判定该证据是否足以表明 CM 的系统运作与 CM 计划相一致。

ACM _ CAP. 3. 9C 引入了一个关于所提供的证据能够表明所有的配置项都是在 CM 系统下进行维护的要求。由于一个配置项即是配置清单上的一项，因此上述的要求就规定配置清单中的所有项都是在 CM 系统下进行维护的。

ACM _ CAP. 4. 11CM 引入了一个关于系统支持 TOE 生成的要求。这就要求 CM 系统提供信息或电子手段来帮助确定在生成 TOE 时使用的是正确的配置项。

ACM _ CAP. 1　版本号

目的：

要求使用一个唯一的参照号，以确保在 TOE 的哪一个样品被评估方面没有歧义。给 TOE 标记上其参照号以确保 TOE 用户可以知道他们所使用的是哪一个 TOE 实物。

依赖关系：

无依赖关系。

开发者行为元素：

ACM _ CAP. 1. 1D 开发者应为 TOE 提供一个参照号。

证据的内容和形式元素：

ACM _ CAP. 1. 1C　TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM _ CAP. 1. 2C　应该给 TOE 标记上其参照号。

评估者行为元素：

ACM _ CAP. 1. 1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ CAP. 2　配置项

目的：

要求使用一个唯一的参照号，以确保在评估 TOE 的实物方面没有歧义。给 TOE 标记上其参照号以确保 TOE 用户可以知道他们所使用的是哪一个 TOE 实物。

配置项的唯一标识可以使我们对 TOE 的组成有更清楚的理解，从而有助于确定哪些配置项满足 TOE 评估要求。

依赖关系：

无依赖关系。

开发者行为元素：

ACM _ CAP. 2. 1D 开发者应为 TOE 提供一个参照号。

ACM _ CAP. 2. 2D **开发者应使用 CM 系统。**

ACM _ CAP. 2. 3D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ CAP. 2. 1C TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM _ CAP. 2. 2C 应该给 TOE 标记上其参照号。

ACM _ CAP. 2. 3C CM 文档应包括一个配置清单。

ACM _ CAP. 2. 4C 配置清单应描述组成 TOE 的配置项。

ACM _ CAP. 2. 5C CM 文档应描述用以唯一标识配置项的方法。

ACM _ CAP. 2. 6C CM 系统应唯一标识所有配置项。

评估者行为元素：

ACM _ CAP. 2. 1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ CAP. 3 授权控制

目的：

要求使用一个唯一的参照号，以确保在评估 TOE 的实物方面没有歧义。给 TOE 标记上其参照号以确保 TOE 用户可以知道他们所使用的是哪一个 TOE 实物。

配置项的唯一标识可以使我们对 TOE 的组成有更清楚的理解，从而有助于确定哪些配置项满足 TOE 评估要求。

提供控制机制以确保不会对 TOE 进行未授权的修改，并保护 CM 系统的正确功能和使用，有助于维护 TOE 的完整性。

依赖关系：

ACM _ SCP. 1 TOE CM 范围

ALC _ DVS. 1 安全措施标识

开发者行为元素：

ACM _ CAP. 3. 1D 开发者应为 TOE 提供一个参照号。

ACM _ CAP. 3. 2D 开发者应使用 CM 系统。

ACM _ CAP. 3. 3D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ CAP. 3. 1C TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM _ CAP. 3. 2C 应该给 TOE 标记上其参照号。

ACM _ CAP. 3. 3C CM 文档应包括一个配置清单**和一个 CM 计划。**

ACM _ CAP. 3. 4C 配置清单应描述组成构 TOE 的配置项。

ACM _ CAP. 3. 5C CM 文档应描述用以唯一标识配置项的方法。

ACM _ CAP. 3. 6C CM 系统应唯一标识所有配置项。

ACM _ CAP. 3. 7C CM 计划应描述 CM 系统是如何使用的。

ACM _ CAP. 3. 8C 证据应该论证 CM 系统的运作与 CM 计划相一致。

ACM _ CAP. 3. 9C CM 文档应提供证据以证明在 CM 系统下有效地维护了所有的配置项。

ACM _ CAP. 3. 10C CM 系统应提供措施使得对配置项只能进行授权修改。

评估者行为元素：

ACM _ CAP.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ CAP.4 产生支持和接受程序

目的：

要求使用一个唯一的参照号，以确保在评估 TOE 的实物方面没有歧义。给 TOE 标记上其参照号以确保 TOE 用户可以知道他们所使用的是哪一个 TOE 实物。

配置项的唯一标识可以使我们对 TOE 的组成有更清楚的理解，从而有助于确定哪些配置项满足 TOE 评估要求

提供控制机制，以确保不会对 TOE 进行未授权的修改，并保护 CM 系统的正确功能和使用，有助于维护 TOE 的完整性。

接受程序的目的是确认对配置项的任何建立和修改都是已授权的。

依赖关系：

ACM _ SCP.1 TOE CM 范围

ALC _ DVS.1 安全措施标识

开发者行为元素：

ACM _ CAP.4.1D 开发者应为 TOE 提供一个参照号。

ACM _ CAP.4.2D 开发者应使用 CM 系统。

ACM _ CAP.4.3D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ CAP.4.1C TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM _ CAP.4.2C 应该给 TOE 标记上其参照号。

ACM _ CAP.4.3C CM 文档应包括一个配置清单、一个 CM 计划**和一个接受计划**。

ACM _ CAP.4.4C 配置清单应描述组成 TOE 的配置项。

ACM _ CAP.4.5C CM 文档应描述用以唯一标识配置项的方法。

ACM _ CAP.4.6C CM 系统应唯一标识所有配置项。

ACM _ CAP.4.7C CM 计划应描述 CM 系统是如何使用的。

ACM _ CAP.4.8C 证据应该论证 CM 系统的运作与 CM 计划相一致。

ACM _ CAP.4.9C CM 文档应提供证据以证明在 CM 系统下有效地维护了所有的配置项。

ACM _ CAP.4.10C CM 系统应提供措施使得对配置项只能进行授权修改。

ACM _ CAP.4.11C CM 系统应支持 TOE 的产生。

ACM _ CAP.4.12C 接受计划应描述用来接受修改过的或新建的作为 TOE 一部分的配置项的程序。

评估者行为元素：

ACM _ CAP.4.1E 评估者应确认所提供的信息满足证据的内容和形式元素的所有要求。

ACM _ CAP.5 高级支持

目的：

要求使用一个唯一的参照号，以确保在评估 TOE 的实物方面没有歧义。给 TOE 标记上其参照号以确保 TOE 用户可以知道他们所使用的是哪一个 TOE 实物。

配置项的唯一标识可以使我们对 TOE 的组成有更清楚的理解，从而有助于确定哪些配置项满足 TOE 评估要求。

提供控制机制，以确保了不会对 TOE 进行未授权的修改，并保护 CM 系统的正确功能性和使用，有助于维护 TOE 的完整性。

接受程序的目的是确认对配置项的任何建立和修改都是已授权的。

集成程序有助于确保由一组受管理的配置项生成一个 TOE 的过程是以授权的方式正确进行的。

要求 CM 系统有能力标识用于生成 TOE 的材料的主拷贝，这有助于确保可以通过适当的技术的、物理的和程序上的安全措施来保护这些材料的完整性。

依赖关系：

ACM _ SCP.1 TOE CM 范围

ALC _ DVS.2 安全措施充分性

开发者行为元素：

ACM _ CAP.5.1D 开发者应为 TOE 提供一个参照号。

ACM _ CAP.5.2D 开发者应使用 CM 系统。

ACM _ CAP.5.3D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ CAP.5.1C TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM _ CAP.5.2C 应该给 TOE 标记上其参照号。

ACM _ CAP.5.3C CM 文档应包括一个配置清单、一个 CM 计划、一个接受计划和集成程序。

ACM _ CAP.5.4C 配置清单应描述组成 TOE 的配置项。

ACM _ CAP.5.5C CM 文档应描述用以唯一标识配置项的方法。

ACM _ CAP.5.6C CM 系统应唯一标识所有配置项。

ACM _ CAP.5.7C CM 计划应描述 CM 系统是如何使用的。

ACM _ CAP.5.8C 证据应该论证 CM 系统的运作与 CM 计划相一致。

ACM _ CAP.5.9C CM 文档应提供证据以证明在 CM 系统下有效地维护了所有的配置项。

ACM _ CAP.5.10C CM 系统应提供措施使得对配置项只能进行授权修改。

ACM _ CAP.5.11C CM 系统应支持 TOE 的产生。

ACM _ CAP.5.12C 接受计划应描述用来接受修改过的或新建的作为 TOE 一部分的配置项的程序。

ACM _ CAP.5.13C 集成程序应描述在 TOE 制造过程中如何使用 CM 系统。

ACM _ CAP.5.14C CM 系统应要求负责将某个配置项接受到 CM 中的人不是开发此配置项的人。

ACM _ CAP.5.15C CM 系统应清楚地标识组成 TSF 的配置项。

ACM _ CAP.5.16C CM 系统应支持所有对 TOE 修改的审计，最起码在审计迹中要包括源发者、日期、时间等信息。

ACM _ CAP.5.17C CM 系统应有能力标识用于生成 TOE 的所有材料的主拷贝。

ACM _ CAP.5.18C CM 文档应论证 CM 系统的使用以及在开发中所使用的安全措施，都只允许对 TOE 作授权修改。

ACM _ CAP.5.19C CM 文档应论证集成程序的使用，能够确保 TOE 的生成是以授权的方式正确执行的。

ACM _ CAP.5.20C CM 文档应论证 CM 系统足以确保负责将某配置项接受到 CM 中的人不是开发这一配置项的人。

ACM _ CAP.5.21C CM 文档应证明接受程序对所有配置项的修改都提供了充分而适当的复查。

评估者行为元素：

ACM _ CAP.5.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

9.3 CM 范围(ACM _ SCP)

目的：

这一子类的目的是确保 CM 系统跟踪所有必需的 TOE 配置项。这样有助于确保这些配置项的完整性是受 CM 系统能力保护的。

本子类的目的包括以下这些方面：

a) 确保 TOE 的实现表示受跟踪；

b) 确保包括问题报告在内的所有必需的文档，在开发和运行过程中都受跟踪；

c) 确保配置选项(例如编译器开关)受跟踪；

d) 确保开发工具受跟踪。

组件分级：

本子类的组件分级是依据以下这些由 CM 系统进行跟踪的因素：TOE 实现表示；设计文档；测试文档；用户文档；管理员文档；CM 文档；安全缺陷以及开发工具。

应用注释：

ACM _ SCP.1.1C 引入了 CM 系统跟踪 TOE 的实现表示的要求。TOE 实现表示指的是组成物理 TOE 的所有硬件、软件和固件。就纯软件 TOE 而言，实现表示可能只包括源代码和目标代码。

ACM _ SCP.1.1C 还引入了 CM 系统跟踪 CM 文档的要求。CM 文档包括 CM 计划以及组成 CM 系统的任何工具的现行版本相关信息。

ACM _ SCP.2.1C 引入了 CM 系统跟踪安全缺陷的要求。这就需要一些有关以前的安全缺陷和如何解决它们的信息，以及关于现行安全缺陷的一些详细信息。

ACM SCP.3.1C 引入了 CM 系统跟踪开发工具和其他相关信息的要求。开发工具的示例有编程语言和编译器。开发工具相关信息的示例有与 TOE 生成项(诸如编译器选项、安装/生成选项、组装选项)有关的信息。

ACM _ SCP.1 TOE CM 范围

目的：

一个 CM 系统只能控制处于 CM 下的那些项的改变。将 TOE 实现表示、设计文档、测试文档、用户文档、管理员文档和 CM 文档置于 CM 之下，可以确保它们的修改是在一个正确授权的可控制方式下进行的。

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ACM _ SCP.1.1D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ SCP.1.1C CM 文档应说明 CM 系统至少能跟踪以下几项：TOE 实现表示，设计文档，测试文档，用户文档，管理员文档和 CM 文档。

ACM _ SCP.1.2C CM 文档应描述 CM 系统是如何跟踪配置项的。

评估者行为元素：

ACM _ SCP.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ SCP.2 跟踪 CM 范围问题

目的：

一个 CM 系统只能控制处于 CM 下的那些项的改变。将 TOE 实现表示、设计文档、测试文档、用户文档、管理员文档和 CM 文档置于 CM 之下，可以确保它们的修改是在一个正确授权的可控制方式下进行的。

在 CM 下跟踪安全缺陷能确保不会丢失或遗忘安全缺陷，和允许开发者从跟踪安全缺陷的过程中找到解决办法。

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ACM _ SCP.2.1D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ SCP.2.1C CM 文档应说明 CM 系统至少能跟踪以下几项：TOE 实现表示，设计文档，测试文档，用户文档，管理员文档，CM 文档**和安全缺陷**。

ACM _ SCP.2.2C CM 文档应描述 CM 系统是如何跟踪配置项的。

评估者行为元素：

ACM _ SCP.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ACM _ SCP.3 CM 范围开发工具

目的：

一个 CM 系统只能控制处于 CM 下的那些项的改变。将 TOE 实现表示、设计文档、测试文档、用户文档、管理员文档和 CM 文档置于 CM 之下，可以确保它们的修改是在一个正确授权的可控制方式下进行的。

在 CM 下跟踪安全缺陷能确保不会丢失或遗忘安全缺陷，和允许开发者从跟踪安全缺陷的过程中找到解决办法。

开发工具对于确保产生 TOE 的优质版本十分重要。因此，对这些工具的修改进行控制是很重要的。

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ACM _ SCP.3.1D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM _ SCP.3.1C CM 文档应说明 CM 系统至少能跟踪以下几项：TOE 实现表示，设计文档，测试文档，用户文档，管理员文档，CM 文档，安全缺陷**以及开发工具和相关信息**。

ACM _ SCP.3.2C CM 文档应描述 CM 系统是如何跟踪配置项的。

评估者行为元素：

ACM _ SCP.2.1E 评估者应确认所提供的信息满足证据的内容和表述的所有要求。

10 ADO 类：交付和运行

交付和运行为 TOE 的正确交付、安装、生成和启动规定了要求。

图 10.1 给出了该类中包含的子类以及子类内组件的层次结构。

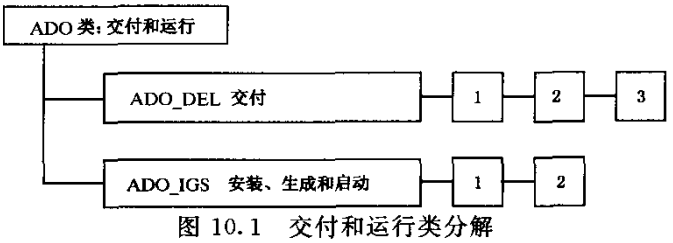

图 10.1 交付和运行类分解

10.1 交付(ADO _ DEL)

目的：

交付要求需要系统控制以及交付设备和程序来提供保证，以确保接收方所接受的 TOE 正是发送者发送的，而没有任何修改。对于有效的交付，收到的东西必需精确地符合 TOE 的主拷贝，这样就避免了篡改现行版本或用错误版本去替代现行版本。

组件分级：

本子类组件的分级，基于对开发者不断提高的要求，使得在交付过程中能够检测和防止对 TOE 的任何修改。

ADO _ DEL.1 交付过程

依赖关系：

无依赖关系。

开发者行为元素：

ADO _ DEL.1.1D **开发者应将把 TOE 及其部分交付给用户的程序文档化。**

ADO _ DEL.1.2D **开发者应使用交付程序。**

证据的内容和形式元素：

ADO _ DEL.1.1C **交付文档应描述，在给用户方分配 TOE 的版本时，用以维护安全所必需的所有程序。**

评估者行为元素：

ADO _ DEL.1.1E **评估者应确认所提供的信息都满足证据的内容和形式的所有要求。**

ADO _ DEL.2 修改监测

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ADO _ DEL.2.1D 开发者应将把 TOE 及其部分交付给用户的程序文档化。

ADO _ DEL.2.2D 开发者应使用交付程序。

证据的内容和形式元素：

ADO _ DEL.2.1C 交付文档应描述，在给用户方分配 TOE 的版本时，用以维护安全所必需的所有程序。

ADO _ DEL.2.2C **交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方收到的版本之间的任何差异。**

ADO _ DEL.2.3C **交付文档应描述如何使用多种程序来检测试图伪装成开发者，甚至在开发者没有向用户方发送任何东西的情况下，向用户方交付 TOE。**

评估者行为元素：

ADO _ DEL.2.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO _ DEL.3 修改防止

依赖关系：

ACM _ CAP.3 授权控制

开发者行为元素：

ADO _ DEL.3.1D 开发者应将把 TOE 及其部分交付给用户的程序文档化。

ADO _ DEL.3.2D 开发者应使用交付程序。

证据的内容和形式元素：

ADO _ DEL.3.1C 交付文档应描述，在给用户方分配 TOE 的版本时，用以维护安全所必需的所有程序。

ADO _ DEL.3.2C 交付文档应描述如何提供多种程序和技术上的措施来防止修改，或检测开发者的主拷贝和用户方收到的版本之间的任何差异。

ADO _ DEL.3.3C 交付文档应描述如何使用多种程序来检测试图伪装成开发者，甚至在开发者没有向用户端发送任何东西的情况下，向用户方交付 TOE。

评估者行为元素：

ADO _ DEL.3.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

10.2 安装、生成和启动(ADO _ IGS)

目的：

安装、生成和启动程序有助于确保 TOE 在开发者所期望的安全方式下进行安装、生成和启动。安装、生成和启动要求需要将处于配置控制下的 TOE 实现表示安全地转换为用户环境下的初始运行。

组件分级：

本子类组件的分级基于 TOE 的生成选项是否被记录。

应用注释：

应该承认，本子类中这些要求的使用将随以下方面不同而不同，譬如 TOE 是一个 IT 产品还是系统，它是否在一个可操作的状态下进行交付，它是否必须由 TOE 的拥有者一方提出等等。对一个给定的 TOE 而言，在关于安装、生成和启动方面，TOE 的开发者和拥有者之间通常负有不同的责任，但有时也有所有的活动在某一方发生的例子。例如，就智能卡而言，所有的安装、生成和启动都在开发者方进行。另一方面，TOE 可能作为 IT 系统以软件的形式交付，此时，安装、生成和启动都在 TOE 的拥有者方进行。

也可能 TOE 在评估开始之前就已经安装好了。在这种情况下就不需要要求和分析安装程序了。

此外，对于生成的要求也只适用于某些 TOE，这些 TOE 能够将其实现表示生成为一个可运行 TOE 的一部分。

安装、生成和启动程序可以存在于单独的文档中，也可以与其他管理员指南结合在一起。本保证子类中的要求都脱离了 AGD _ ADM 子类中的要求而独立进行表述，这主要是由于安装、生成和启动程序都很少使用，很有可能只用一次。

ADO _ IGS.1 安装、生成和启动过程

依赖关系：

AGD _ ADM.1 管理员指南

开发者行为元素：

ADO _ IGS.1.1D 开发者应将 TOE 安全地安装、生成和启动所必要的程序文档化。

证据的内容和形式元素：

ADO _ IGS.1.1C 文档应描述 TOE 安全地安装、生成和启动所必要的步骤。

评估者行为元素：

ADO _ IGS.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO _ IGS.1.2E 评估者应决定安装、生成和启动程序最终产生了安全的配置。

ADO _ IGS.2 日志生成

依赖关系：

AGD _ ADM.1 管理员指南

开发者行为元素：

ADO _ IGS.2.1D 开发者应将 TOE 安全地安装、生成和启动所必要的程序文档化。

证据的内容和形式元素：

ADO _ IGS.2.1C 文档应描述 TOE 安全地安装、生成和启动所必要的步骤。

ADO _ IGS.2.2C **文档应描述能建立一个记录日志的程序，该日志包含用以生成 TOE 的生成选项，这样就有可能正确地确定 TOE 是如何以及何时产生的。**

评估者行为元素：

ADO _ IGS.2.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO _ IGS.2.2E 评估者应决定安装、生成和启动程序最终产生了安全的配置。

11 ADV 类：开发

开发类包括四个子类的要求，这些子类从功能接口到实现表示不同的抽象级别上表示 TSF。开发类也包括一个子类的要求，该子类在各种 TSF 表示之间建立相应的映射，并最终要求论证从最不抽象的表示，通过所有中间表示，到 ST 所提供的 TOE 概要规范之间的对应性关系。此外，还包括了一个子类的关于 TSP 模型以及 TSP、TSP 模型和功能规范之间对应映射的要求。最后，该类还包括一个子类的关于 TSF 内部结构的要求，TSF 的内部结构要求子类覆盖了模块化、层次化以及复杂性最小化等方面。

图 11.1 给出了该类中包含的子类以及子类内组件的层次结构。

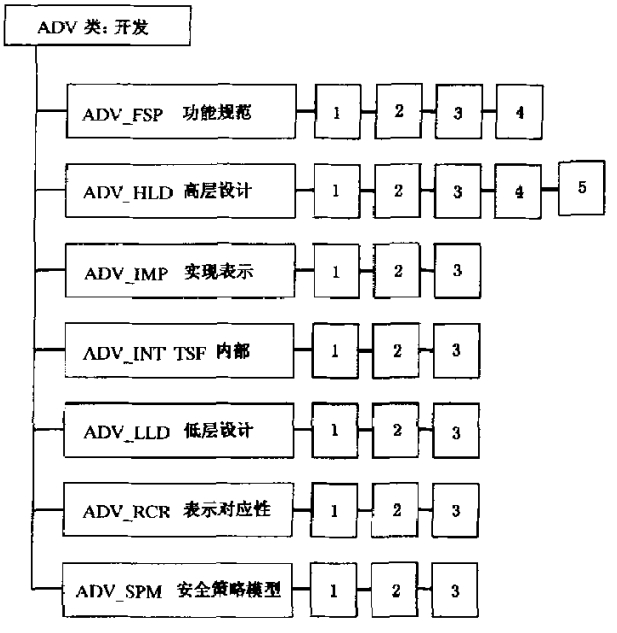

图 11.1 开发类分解

这些子类的明显范例是一个 TSF 的功能规范，将 TSF 分解成子系统，再将子系统分解成模块，说明模块的实现，并且把各分解之间对应性的论证提供来作为证据。各种 TSF 表示要求将被分解到不同的子类中，但仍允许 PP/ST 的作者指明需要哪一个 TSF 表示子集。

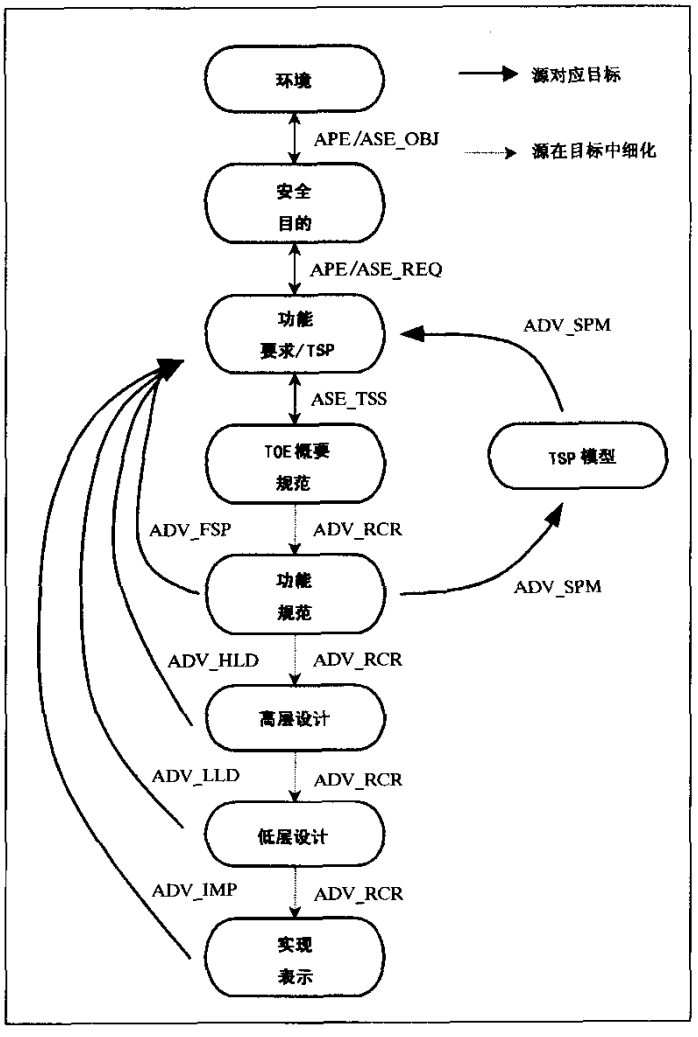

图 11.2 TOE 表示和要求之间的关系

图 11.2 表明各种 TSF 表示和目的之间的关系，以及它们需要满足的要求。如图所示，APE 和 ASE 两类定义了关于功能要求和安全目的之间对应性的要求，以及安全目的和 TOE 预期环境之间对应性的要求。ASE 类也定义安全目的和功能要求与 TOE 概要规范之间对应性的要求。

关于图 11.2 所示的所有其他对应性的要求都在 ADV 类中定义。ADV _ SPM 子类定义 TSP 和 TSP 模型之间对应性的要求，以及 TSP 模型和功能规范之间对应性的要求。ADV _ RCR 子类定义从 TOE 概要规范到实现表示所有可用的 TSF 表示之间对应性的要求。最后，与一个 TSF 表示有关每个保证子类(即 ADV _ FSP、ADV _ HLD、ADV _ LLD 和 ADV _ IMP)定义将该 TSF 表示与功能要求联系起来的要求，这些保证结合起来有助于确保 TOE 安全功能要求都被罗列了出来。从最高层的 TSF 表示到所提供的每个 TSF 表示，总要执行可溯性分析。GB/T 18336 通过依赖于 ADV _ RCR 子类来获得该可溯性要求。在图中没有标出 ADV _ INT 子类，因为它仅仅与 TSF 内部结构相关，并且仅与 TSF 表示的细化过程间接相关。

应用注释：

TOE 安全策略(TSP)是一组规则，它控制在一个 TOE 内如何管理、保护和分配资源，并由 TOE 安

全功能要求来作表述。没有明确地要求开发者提供一个 TSP，因为 TSP 是由 TOE 的安全功能要求，通过安全功能策略(SFP)和其他一些单独的要求元素的一个组合来表述的。

TOE 安全功能(TSF)是指 TSP 的实施所必须依赖的 TOE 的所有部分。TSF 既包括一些直接实施 TSP 的功能，也包括那些虽然不直接实施 TSP，但是以一种更间接的方式来实施 TSP 的功能。

虽然在 ASE _ TSS 子类和本类其他几个子类中的要求需要几个不同的 TSF 表示，但并不一定需要将每一个 TSF 表示分别放在不同的文档中。事实上，可能是这种情况：单文档满足多个 TSF 表示的文档要求，因为需要的是每个 TSF 表示的信息，而不是最终文档结构。当多个 TSF 表示组合在一个单文档里时，开发者应该表明哪个文档满足哪个要求。

在这个类中有三种类型的规范风格：非形式化、半形式化和形式化。功能规范、高层设计、低层设计和 TSP 模型都将使用以上一种或多种规范风格来书写。通过使用一个逐渐增加的形式化程度，来减少这些规范的歧义。

非形式化规范就是像散文一样用自然语言来书写。在这里使用自然语言来作为任何普通口头语言(如荷兰语、英语、法语、德语)中意思的沟通。非形式化规范不像常规语言的传统用法(如文法和句法)一样受一些符号或特殊的限制。虽然没有符号限制，非形式化规范也要求为上下文中的术语定义其意思，除非作为常规用法已认可。

半形式化规范就是用一种受限制的句法语言来书写，并且通常伴随着支持性的解释(非形式化)语句。这里的受限制句法语言可以是一种带有受限制句子结构和具有特殊意义的关键字的自然语言，也可以是图表式的(如数据流图、状态转换图、实体关系图、数据结构图、流程或程序结构图)。不论基于图表还是自然语言，必须用一套规范来定义句法限制。

形式化规范就是用一套基于明确定义的数学概念的符号来书写，并且通常伴随着支持性的解释(非形式化)语句。这些数学概念被用来定义符号的句法和语义，以及支持逻辑推理的证明规则。支持形式化符号的句法和语义规则应该定义如何明确地识别其结构和确定其含义。并且必须有证据表明矛盾不可能产生，和支持符号的所有规则都有定义或者引用。

可以通过以下方式获得有效的保证：确保能够通过 TSF 的每一个表示来跟踪 TSF，和确保 TSP 模型与功能规范相互对应。ADV _ RCR 子类包含了各种 TSF 表示之间对应映射的要求，ADV _ SPM 子类包含了 TSP 模型和功能规范之间对应映射的要求。对应性可以采用非形式化论证、半形式化论证或者形式化证明三种形式来说明。

当要求非形式化地论证对应性时，就意味着只要求一个基础的对应性。对应性方法包括，例如，使用带有指示对应性条目的二维表格，或者使用适当的设计图符号。还可使用指针和对其他文档的引用。

对应性的半形式化论证要求用结构化的处理方法来分析对应性对应性。这种方法应该通过限制在对应性中术语的解释，来减少在非形式化对应性中可能存在的歧义。可使用指针和对其他文档的引用。

对应性的形式化证明要求采用已确定的数学概念来定义形式化符号的句法和语义，以及一些支持逻辑推理的证明规则。安全属性需要用形式化的规范语言来表述，并且需要说明形式化的规范满足这些安全属性。还可使用指针和对其他文档的引用。

ADV _ RCR. *. 1C 元素要求开发者为每一对相邻的 TSF 表示提供证据，以表明在较为抽象的 TSF 表示中，所有相关的安全功能都在较低级抽象的 TSF 表示中被细化。ADV _ FSP. *. 2E，ADV _ HLD. *. 2E，ADV _ LLD. *. 2E 和 ADV _ IMP. *. 2E 等元素都要求评估者确定由该子类要求所表示的 TSF 是 TOE 安全功能要求的一个精确且完备的实例化。为了确定一个 TSF 表示是 TOE 安全功能要求的一个精确的和完备的实例化，希望评估者将开发者在 ADV _ RCR. *. 1C 中所提供的证据作为该判定的一个输入。通过建立 TOE 安全功能要求与链上每个后继 TSF 表示之间的一个对应性关系，这个渐进的过程将最终提供更多的保证，确保最不抽象的 TSF 表示都符合 TOE 安全功能要求，这就是本类的最终目的。如果评估者没有作出将中间级的 TSF 表示回溯到 TOE 的安全功能要求这种对应性判定，那么，试图作出从最不抽象的 TSF 表示回溯到 TOE 的安全功能要求这种对应性判定，就可能会

由于表示的跨度太大而无法正确地进行。最后，根据所要求的 TSF 表示集合，低层设计、高层设计、或者甚至功能规范就是所提供的最不抽象的 TSF 表示，这是完全可能的。

11.1 功能规范(ADV _ FSP)

目的：

功能规范是用户可见接口和 TSF 行为的一个高层描述。它是 TOE 安全功能要求的一个实例化。功能规范须说明所有 TOE 安全功能要求都已被罗列出了。

组件分级：

本子类的组件分级基于功能规范所要求的形式化程度和所提供的 TSF 外部接口的详细程度。

应用注释：

本子类内的 ADV _ FSP. *. 2E 元素定义了这样的一个要求，即评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。这就提供了 TOE 安全功能要求和功能规范之间的直接对应性，以作为 ADV _ RCR 子类所要求的成对对应性的补充。希望评估者利用在 ADV _ RCR 中提供的证据作为该判定的输入，对完备性的要求也将与功能规范的抽象程度有关。

ADV _ FSP. 1. 3C 打算在功能规范中已提供足够的信息，以理解 TOE 安全功能要求是如何被提出来的，并使得 ST 中的测试规范能反映 TOE 安全功能要求。测试无须涵盖在接口产生的所有可能的返回值和错误信息，但是所提供的信息应该解释在成功的情况下和在最一般失败的情况下使用接口的结果。

ADV _ FSP. 2. 3C 引入了一个关于功能接口的完备表示的要求。这将为支持 TOE 的全面测试和脆弱性评定提供必要的细节。

在功能规范形式化程度的上下文中，非形式化、半形式化和形式化三个等级的的划分实际上都是主观的。因此，ADV _ FSP. 1. 1C 和 ADV _ FSP. 2. 1C 也可以满足半形式化或形式化功能规范，假若有非形式化的、适当的解释性文字支持的话。此外，ADV _ FSP. 3. 1C 也能够满足形式化的功能规范。

ADV _ FSP. 1 非形式化功能规范

依赖关系：

ADV _ RCR. 1 非形式化对应性论证

开发者行为元素：

ADV _ FSP. 1. 1D 开发者应当提供功能规范。

证据的内容和形式元素：

ADV _ FSP. 1. 1C 功能规范应当使用非形式化风格来描述 TSF 及其外部接口。

ADV _ FSP. 1. 2C 功能规范应当是内在一致的。

ADV _ FSP. 1. 3C 功能规范应当描述所有外部 TSF 接口的用途与使用方法，适当的时候，要提供影响、例外情况和错误消息的细节。

ADV _ FSP. 1. 4C 功能规范应当完备地表示 TSF。

评估者行为元素：

ADV _ FSP. 1. 1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ FSP. 1. 2E 评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ FSP. 2 完全定义的外部接口

依赖关系：

ADV _ RCR. 1 非形式化对应性论证

开发者行为元素：

ADV _ FSP.2.1D 开发者应当提供功能规范。

证据的内容和形式元素：

ADV _ FSP.2.1C 功能规范应当使用非形式化风格来描述 TSF 及其外部接口。

ADV _ FSP.2.2C 功能规范应当是内在一致的。

ADV _ FSP.2.3C 功能规范应当描述所有外部 TSF 接口的用途与使用方法，适当的时候，要提供所有的影响、例外情况和错误消息的全部细节。

ADV _ FSP.2.4C 功能规范应当完备地表示 TSF。

ADV _ FSP.2.5C 功能规范应当包括 TSF 是完备地表示的基本原理。

评估者行为元素：

ADV _ FSP.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ FSP.2.2E 评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ FSP.3 半形式化功能规范

依赖关系：

ADV _ RCR.1 非形式化对应性论证

开发者行为元素：

ADV _ FSP.3.1D 开发者应当提供功能规范。

证据的内容和形式元素：

ADV _ FSP.3.1C 功能规范应当使用**半形式化**风格来描述 TSF 及其外部接口，**并靠非形式化的、适当的解释性文字来支持**。

ADV _ FSP.3.2C 功能规范应当是内在一致的。

ADV _ FSP.3.3C 功能规范应当描述所有外部 TSF 接口的用途与使用方法，适当的时候，要提供所有的影响、例外情况和错误消息的全部细条。

ADV _ FSP.3.4C 功能规范应当完备地表示 TSF。

ADV _ FSP.3.5C 功能规范应当包括 TSF 是完备地表示的基本原理。

评估者行为元素：

ADV _ FSP.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ FSP.3.2E 评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ FSP.4 形式化功能规范

依赖关系：

ADV _ RCR.1 非形式化对应性论证

开发者行为元素：

ADV _ FSP.4.1D 开发者应当提供功能规范。

证据的内容和形式元素：

ADV _ FSP.4.1C 功能规范应当使用**形式化**风格来描述 TSF 与其外部接口，**并靠非形式化的、适当的解释性文字来支持**。

ADV _ FSP.4.2C 功能规范应当是内在一致的。

ADV _ FSP.4.3C 功能规范应当描述所有外部 TSF 接口的用途与使用方法，适当的时候，要提供所有的影响、例外情况和错误消息的全部细节。

ADV _ FSP.4.4C 功能规范应当完备地表示 TSF。

ADV _ FSP.4.5C 功能规范应当包括 TSF 是完备地表示的基本原理。

评估者行为元素：

ADV _ FSP.4.1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ FSP.4.2E　评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

11.2　高层设计(ADV _ HLD)

目的：

一个 TOE 的高层设计在主要的结构单元(即子系统)和将这些单元同所提供的功能相联系方面提供 TSF 的一种描述。高层设计要求试图提供这样的保证，即 TOE 提供了适当的体系结构来实现 TOE 安全功能要求。

高层设计将功能规范细化成子系统。对于 TSF 的每一个子系统，高层设计描述其用途和功能，并且标识出包含在子系统中的安全功能。高层设计也定义所有子系统之间的相互关系。这些相互关系将适当地被表示成数据流、控制流等的外部接口。

组件分级：

本子类的组件分级基于高层设计所要求的形式化程度和所提供的接口规范的详细程度。

应用注释：

希望开发者按子系统来描述 TSF 的设计。术语“子系统”在这里是指把 TSF 分解成相对较小的几部分。虽然不要求开发者实际上建立“子系统”，但是希望开发者表示出类似的分解级别。例如，一个设计可能类似地用“层”、“域”或“服务”来分解。

术语“安全功能性”用来表示一个子系统执行的一组操作，这些操作有助于 TOE 实现其安全功能。造成这种差别是因为设计构造，如子系统和模块，不一定与具体的安全功能相关联。虽然一个给定的子系统直接对应于某个或者甚至是几个安全功能，也有可能多个子系统组合起来才能实现一个单独的安全功能。

术语“TSP 实施子系统”指的是实施 TSP 的一个子系统，既可以是直接地也可以是间接地。

本子类内的 ADV _ HLD. *.2E 元素定义了这样的一个要求，即评估者确定高层设计是 TOE 安全功能的一个精确且完备的实例化。这就提供了 TOE 安全功能要求和高层设计之间的直接对应性，这也是对 ADV _ RCR 子类所要求的成对对应性的补充。希望评估者利用在 ADV _ RCR 中提供的证据作为该判定的输入，对完备性的要求也将与高层设计的抽象程度有关。

ADV _ HLD.3.8C 引入了关于子系统接口的完备表示的一个要求。这将为支持 TOE 的全面测试(利用 ATE _ DPT 中的组件)和脆弱性评定提供必要的细节。

在高层设计形式化程度的上下文中，非形式化、半形式化和形式化三个等级的的划分实际上都是主观的。因此，ADV _ HLD.1.1C 和 ADV _ HLD.2.1C 也可以满足半形式化或形式化的高层设计，ADV _ HLD.3.1C 和 ADV _ HLD.4.1C 也能够满足形式化的高层设计。

ADV _ HLD.1　描述性高层设计

依赖关系：

ADV _ FSP.1　非形式化功能规范

ADV _ RCR.1　形式化对应性论证

开发者行为元素：

ADV _ HLD.1.1D　开发者应当提供 TSF 的高层设计。

证据的内容和形式元素：

ADV _ HLD.1.1C 高层设计的表示应当是非形式化的。
ADV _ HLD.1.2C 高层设计应当是内在一致的。
ADV _ HLD.1.3C 高层设计应当按子系统来描述 TSF 的结构。
ADV _ HLD.1.4C 高层设计应当描述 TSF 的每一个子系统所提供的安全功能。
ADV _ HLD.1.5C 高层设计应当标识 TSF 所要求的任何基础性硬件、固件或软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。
ADV _ HLD.1.6C 高层设计应当标识 TSF 子系统的所有接口。
ADV _ HLD.1.7C 高层设计应当标识 TSF 子系统的哪些接口是外部可见的。
评估者行为元素：
ADV _ HLD.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV _ HLD.1.2E 评估者应当决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ HLD.2 安全加强的高层设计
依赖关系：
ADV _ FSP.1 非形式化功能规范
ADV _ RCR.1 形式化对应性论证
开发者行为元素：
ADV _ HLD.2.1D 开发者应当提供 TSF 的高层设计。
证据的内容和形式元素：
ADV _ HLD.2.1C 高层设计的表示应当是非形式化的。
ADV _ HLD.2.2C 高层设计应当是内在一致的。
ADV _ HLD.2.3C 高层设计应当按子系统来描述 TSF 的结构。
ADV _ HLD.2.4C 高层设计应当描述 TSF 的每一个子系统所提供的安全功能。
ADV _ HLD.2.5C 高层设计应当标识 TSF 所要求的任何基础性的硬件、固件或软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。
ADV _ HLD.2.6C 高层设计应当标识 TSF 子系统的所有接口。
ADV _ HLD.2.7C 高层设计应当标识 TSF 子系统的哪些接口是外部可见的。
ADV _ HLD.2.8C 高层设计应当描述 TSF 子系统所有接口的用途与使用方法，并适当提供影响、例外情况和错误消息的细节。
ADV _ HLD.2.9C 高层设计应当描述把 TOE 分成 TSP-实施和其他子系统的这种分离。
评估者行为元素：
ADV _ HLD.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV _ HLD.2.2E 评估者应当决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ HLD.3 半形式化高层设计
依赖关系：
ADV _ FSP.3 半形式化的功能规范
ADV _ RCR.2 半形式化的对应性论证
开发者行为元素：
ADV _ HLD.3.1D 开发者应当提供 TSF 的高层设计。
证据的内容和形式元素：
ADV _ HLD.3.1C 高层设计表示应当是半形式化的。
ADV _ HLD.3.2C 高层设计应当是内在一致的。

ADV _ HLD.3.3C 高层设计应当按子系统来描述 TSF 的结构。
ADV _ HLD.3.4C 高层设计应当描述 TSF 的每一个子系统所提供的安全功能。
ADV _ HLD.3.5C 高层设计应当标识 TSF 所要求的任何基础性的硬件、固件或软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。
ADV _ HLD.3.6C 高层设计应当标识 TSF 子系统的所有接口。
ADV _ HLD.3.7C 高层设计应当标识 TSF 子系统的哪些接口是外部可见的。
ADV _ HLD.3.8C 高层设计应当描述 TSF 子系统所有接口的用途与使用方法，并提供所有的影响、例外情况和错误消息的全部细节。
ADV _ HLD.3.9C 高层设计应当描述把 TOE 分成 TSP-实施和其他子系统的这种分离。
评估者行为元素
ADV _ HLD.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV _ HLD.3.2E 评估者应当决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ HLD.4 半形式化高层解释

依赖关系：
ADV _ FSP.3 半形式化功能规范
ADV _ RCR.2 半形式化对应性论证
开发者行为元素：
ADV _ HLD.4.1D 开发者应当提供 TSF 的高层设计。
证据的内容和形式元素：
ADV _ HLD.4.1C 高层设计表示应当是半形式化的。
ADV _ HLD.4.2C 高层设计应当是内在一致的。
ADV _ HLD.4.3C 高层设计应当按子系统来描述 TSF 的结构。
ADV _ HLD.4.4C 高层设计应当描述 TSF 的每一个子系统所提供的安全功能。
ADV _ HLD.4.5C 高层设计应当标识 TSF 所要求的任何基础性的硬件、固件和软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。
ADV _ HLD.4.6C 高层设计应当标识 TSF 子系统的所有接口。
ADV _ HLD.4.7C 高层设计应当标识 TSF 子系统的哪些接口是外部可见的。
ADV _ HLD.4.8C 高层设计应当描述 TSF 子系统所有接口的用途与使用方法，并提供所有的影响、例外情况和错误消息的全部细节。
ADV _ HLD.4.9C 高层设计应当描述把 TOE 分成 TSP-实施和其他子系统的这种分离。
ADV _ HLD.4.10C **高层设计应当证明所标识的分离方法，包括任何保护机制，是足以确保完全而有效地将 TSP-实施功能同非 TSP-实施功能分开。**
ADV _ HLD.4.11C **高层设计应当证明 TSF 机制足以实现在高层设计中所标识的安全功能。**
评估者行为元素：
ADV _ HLD.4.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV _ HLD.4.2E 评估者应当决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ HLD.5 形式化高层设计

依赖关系：
ADV _ FSP.4 形式化功能规范
ADV _ RCR.3 形式化对应性论证
开发者行为元素：

ADV _ HLD.5.1D 开发者将提供 TSF 的高层设计。

证据的内容和形式元素：

ADV _ HLD.5.1C 高层设计的表示应当是形式化的。

ADV _ HLD.5.2C 高层设计应当是内在一致的。

ADV _ HLD.5.3C 高层设计应当按子系统来描述 TSF 的结构。

ADV _ HLD.5.4C 高层设计应当描述 TSF 的每一个子系统提供的安全功能。

ADV _ HLD.5.5C 高层设计应当标识 TSF 所要求的任何基础性的硬件、固件和软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。

ADV _ HLD.5.6C 高层设计应当标识 TSF 子系统的所有接口。

ADV _ HLD.5.7C 高层设计应当标识 TSF 子系统的哪些接口是外部可见的。

ADV _ HLD.5.8C 高层设计应当描述 TSF 子系统所有接口的用途与使用方法，并提供所有的影响、例外情况和错误消息的全部细节。

ADV _ HLD.5.9C 高层设计应当描述把 TOE 分成 TSP-实施和其他子系统的这种分离。

ADV _ HLD.5.10C 高层设计应当证明所标识的分离方法，包括任何保护机制，是足以确保完全而有效地将 TSP-实施功能同非 TSP-实施功能分开。

ADV _ HLD.5.11C 高层设计应当证明 TSF 机制足以实现在高层设计中所标识的安全功能。

评估者行为元素：

ADV _ HLD.5.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ HLD.5.2E 评估者应当决定功能规范是 TOE 安全功能要求的一个精确且完备的实例化。

11.3 实现表示(ADV _ IMP)

目的：

以源代码、固件或硬件图样等形式描述实现表示时，可以获得详细的 TSF 内部工作情况来支持分析。

组件分级：

本子类的组件分级基于所提供的实现表示的完备性和结构。

应用注释：

实现表示用于表达 TSF 的最不抽象表示的概念，尤其是那种不需进一步在设计上细化就用来建立 TSF 的表示。被编译的源代码或用来建造实际硬件的硬件图样都是部分实现表示的例子。

可能评估者会利用实现表示来直接支持其他评估活动(如脆弱性分析、测试范围分析或额外的评估者测试的识别)。希望 PP/ST 的作者会选择这样的组件，它要求实现是足够完备和彻底的，以至于可提出需要包括在 PP/ST 中的所有其他要求。

ADV _ IMP.1 TSF 子集的实现

应用注释：

ADV _ IMP.1.1D 要求开发者提供 TSF 子集的实现表示。其目的是通过对至少 TSF 某一部分的访问，为评估者提供机会来检查 TOE 这些部分的实现表示，这里的检查能够对所使用机制增进了解，增加保证。提供实现表示范例，同时也允许评估者对可追溯性证据进行抽样，以便获得细化所用方法的保证，并且评定实现表示本身的陈述。

ADV _ IMP.1.2E 元素定义了这样的要求，即评估者确定最不抽象的 TSF 表示是 TOE 安全功能的一个精确且完备的实例化。这就提供了 TOE 安全功能要求和最不抽象 TSF 表示之间的直接对应性，

作为 ADV _ RCR 子类所要求的成对对应性的补充。希望评估者利用 ADV _ RCR 所提供的证据作为该判定的输入条件。本组件中最不抽象的 TSF 表示，是所提供的实现表示和部分与所提供实现表示不一致的低层设计二者的集合。

依赖关系：

ADV _ LLD.1　描述性低层设计

ADV _ RCR.1　非形式化对应性论证

ALC _ TAT.1　明确定义的开发工具

开发者行为元素：

ADV _ IMP.1.1D　开发者应当为选定的 TSF 子集提供实现表示。

证据的内容和形式元素：

ADV _ IMP.1.1C　实现表示应当无歧义而且详细地定义 TSF，使得无须进一步设计就能生成 TSF。

ADV _ IMP.1.2C　实现表示应当是内在一致的。

评估者行为元素：

ADV _ IMP.1.1E　评估者应当确认提供的信息满足证据的内容和形式的所有要求。

ADV _ IMP.1.2E　评估者应当决定所提供的最不抽象的 TSF 表示是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ IMP.2　TSF 的实现

应用注释：

ADV _ IMP.2.2E 元素定义了这样的要求，即评估者确定实现表示是 TOE 安全功能的一个精确且完备的实例化。这就提供了 TOE 安全功能要求和实现表示之间的直接对应性，作为 ADV _ RCR 子类所要求的成对对应性的补充。希望评估者利用 ADV _ RCR 所提供的证据作为该判定的输入条件。

依赖关系：

ADV _ LLD.1　描述性低层设计

ADV _ RCR.1　非形式化对应性论证

ALC _ TAT.1　明确定义的开发工具

开发者行为元素：

ADV _ IMP.2.1D　开发者应当为**整个 TSF** 提供实现表示。

证据的内容和形式元素：

ADV _ IMP.2.1C　实现表示应当无歧义而且详细地定义 TSF，使得无须进一步设计就能生成 TSF。

ADV _ IMP.2.2C　实现表示应当是内在一致的。

ADV _ IMP.2.3C　实现表示应当描述实现各部分之间的关系。

评估者行为元素：

ADV _ IMP.2.1E　评估者应该确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ IMP.2.2E　评估者应该决定**实现表示**是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ IMP.3　TSF 的结构化实现

应用注释：

ADV _ IMP.2.2E 元素定义了这样的要求，即评估者确定实现表示是 TOE 安全功能的一个精确而完备的实例化。这就提供了 TOE 安全功能要求和实现表示之间的直接对应性，作为 ADV _ RCR 子类所要求的成对对应性的补充。希望评估者利用 ADV _ RCR 所提供的证据作为该判定的输入条件。

依赖关系：

ADV _ INT.1　模块化

ADV _ LLD.1 描述性低层设计
ADV _ RCR.1 非形式化对应性论证
ALC _ TAT.1 明确定义的开发工具

开发者行为元素：

ADV _ IMP.3.1D 开发者应当为整个 TSF 提供实现表示。

证据的内容和形式元素：

ADV _ IMP.3.1C 实现表示应当无歧义而且详细地定义 TSF，使得无须进一步设计就能生成 TSF。
ADV _ IMP.3.2C 实现表示应当是内在一致的。
ADV _ IMP.3.3C 实现表示应当描述实现各部分之间的关系。
ADV _ IMP.3.4C **实现表示应当被构造成一些小的且易于理解的部件。**

评估者行为元素：

ADV _ IMP.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV _ IMP.3.2E 评估者应当决定实现表示是 TOE 安全功能要求的一个精确且完备的实例化。

11.4 TSF 内部（ADV _ INT）

目的：

本子类提出了 TSF 的内部结构。提出了有关模块化、层次化（依照抽象度分层，最少循环依赖）、策略实施机制的复杂性最小化、TSF 中非 TSP-实施功能性的数目最小化等方面的要求，这样 TSF 就简单到可分析了。

模块化的设计减少了 TSF 各部分之间的相互依赖关系，这样就降低了由于一个模块的更改或错误而影响整个 TOE 的风险。因此，一个模块的设计，就提供了确定 TSF 其他元素之间相互作用范围的基础，更加保证了不会产生未预见的影响，并且也提供了设计和评估测试套件的基础。

层次化和 TSP-实施功能性的简单设计的使用，减小了 TSF 的复杂性。从而使得 TSF 更易于理解，更加保证了 TOE 的安全功能要求都在实现中被精确且完备地实例化。

减少 TSF 中不实施 TSP 的功能性的数目，就减少了 TSF 中缺陷存在的可能性。模块化与层次化相结合，就使评估者仅仅注意那些对 TSP 实施而言必要的功能。

设计复杂性的最小化有助于保证代码可理解——TSF 中的代码越简单，TSF 的设计越容易理解。设计复杂性的最小化是参照确认机制的关键特性。

组件分级：

本子类的组件分级，基于结构的数目和所要求的最小化。

应用注释：

术语“TSF 的部分”用来表示那些带有不同粒度的 TSF 部分，其粒度基于可用的 TSF 表示。功能规范允许根据接口来标识，高层设计允许根据子系统来标识，低层设计允许根据模块来标识，实现表示允许根据实现单元来标识。

ADV _ INT.2.5C 和 ADV _ INT.3.5C 元素提出各层之间相互作用的最小化。然而，在各层之间存在相互作用仍是允许的，但在这种情况下，要求开发者论证这种相互作用是必要的，而且不能合理地避免。

ADV _ INT.2.6C 通过要求实施在 TSP 中标识的访问控制或信息流控策略的部分 TSF 复杂性的最小化，引入一个参照监视器的概念。ADV _ INT.3.6C 通过要求整个 TSF 复杂性的最小化进一步发展参照监视器这个概念。

本子类组件中的几个元素涉及到结构化描述。这种结构化描述与低层设计在抽象级别上有些相似，

因为它与 TSF 的模块密切相关。然而低层设计描述的是 TSF 模型的设计，结构化描述的目的是在适用时提供模块化、层次化和 TSF 复杂性最小化的证据。低层设计和实现表示都要求遵照结构化描述，以保证这些 TSF 表示具有所要求的模块化、层次化和复杂性最小化。

ADV _ INT.1　模块化

依赖关系：

ADV _ IMP.1　TSF 子集的实现

ADV _ LLD.1 描述性低层设计

开发者行为元素：

ADV _ INT.1.1D　开发者应当以模块方式设计和构建 TSF，以避免设计模块之间出现不必要的交互作用。

ADV _ INT.1.2D　开发者应当提供一种结构化描述。

证据的内容和形式元素：

ADV _ INT.1.1C　结构化描述应当标识 TSF 的模块。

ADV _ INT.1.2C　结构化描述应当描述每一个 TSF 模块的用途、接口、参数和影响。

ADV _ INT.1.3C　结构化描述应当描述 TSF 设计是如何使得独立的模块间避免不必要的交互作用。

评估者行为元素：

ADV _ INT.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ INT.1.2E　评估者应当决定低层设计和实现表示都是遵循结构化描述的。

ADV _ INT.2　复杂性降低

应用注释：

这一组件通过要求实施在 TSP 中标识的访问控制或信息流控策略的 TSF 部分复杂性最小化，引入一个参照监视器的概念。

依赖关系：

ADV _ IMP.1　TSF 子集的实现

ADV _ LLD.1 描述性低层设计

开发者行为元素：

ADV _ INT.2.1D　开发者应当以模块方式设计和构建 TSF，以避免设计模块之间出现不必要的交互作用。

ADV _ INT.2.2D　开发者应当提供一种结构化描述。

ADV _ INT.2.3D　开发者应当以分层方式设计和构建 TSF，以最小化设计层次之间的交互作用。

ADV _ INT.2.4D　开发者应当以以下方式设计和构建 TSF，即最小化实施任何访问控制或信息流控制策略的 TSF 部分的复杂性。

证据的内容和形式元素：

ADV _ INT.2.1C　结构化描述应当识别 TSF 的模块，**并应指明 TSF 的哪些部分是实施访问控制或信息流控制策略的。**

ADV _ INT.2.2C　结构化描述应当描述每一个 TSF 模块的用途、接口、参数和影响。

ADV _ INT.2.3C　结构化描述应当描述 TSF 设计是如何使得独立的模块间避免不必要的交互作用。

ADV _ INT.2.4C　结构化描述应描述分层结构。

ADV _ INT.2.5C　结构化描述应说明如何使交互作用最小化，并证明所残留的交互作用是正确的。

ADV _ INT.2.6C　结构化描述应描述那些实施访问控制或信息流控制策略的 TSF 部分是如何被构建，从而达到最小复杂性。

评估者行为元素：

ADV _ INT. 2. 1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ INT. 2. 2E 评估者应当决定低层设计和实现表示都是遵循结构化描述的。

ADV _ INT. 3　复杂性最小化

应用注释：

这一组件要求全面论证参照监视器的属性“简单到足以加以分析”。当这个组件与功能要求 FPT _ RVM. 1 和 FPT _ SEP. 3 两组件结合在一起时，参照监视器这一概念是可完全实现的。

依赖关系：

ADV _ IMP. 2　TSF 实现

ADV _ LLD. 1 描述性低层设计

开发者行为元素：

ADV _ INT. 3. 1D　开发者应当以模块方式设计和构建 TSF，以避免设计模块之间出现不必要的交互作用。

ADV _ INT. 3. 2D 开发者应当提供一种结构化描述。

ADV _ INT. 3. 3D　开发者应当以分层的方式设计和构建 TSF，以最小化设计层次之间的交互作用。

ADV _ INT. 3. 4D　开发者应当以最小化整个 TSF 复杂性的方式设计和构建 TSF。

ADV _ INT. 3. 5D　开发者应当把实施访问控制或信息流控制策略的 TSF 部分设计和构建得足够简单以至于可以分析。

ADV _ INT. 3. 6. D　开发者应当确保那些其目的与 TSF 无关的功能都已从 TSF 模块中排斥出去。

证据的内容和形式元素：

ADV _ INT. 3. 1C　结构化描述应当识别 TSF 的模块，并应指明 TSF 的哪些部分是实施访问控制或信息流控策略的。

ADV _ INT. 3. 2C　结构化描述应当描述每一个 TSF 模块的用途、接口、参数和影响。

ADV _ INT. 3. 3C　结构化描述应当描述 TSF 设计是如何使得独立的模块间避免不必要的交互作用。

ADV _ INT. 3. 4C　结构化描述应描述分层结构。

ADV _ INT. 3. 5C　结构化描述应说明如何使交互作用最小化，并证明所残留的交互作用是正确的。

ADV _ INT. 3. 6C　结构化描述应描述整个 TSF 是如何被构建，从而达到最小复杂性。

ADV _ INT3. 7C　结构化描述应当证明 TSF 中对任何非 TSP-实施模块的包含关系都是正确的。

评估者行为元素：

ADV _ INT. 3. 1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ INT. 3. 2E　评估者应当决定低层设计和实现表示都是遵循结构化描述的。

ADV _ INT3. 3E　评估者应当确认实施任何访问控制和信息流控制策略的 TSF 部分都已经足够简单，以至于可加以分析。

11.5　低层设计(ADV _ LLD)

目的：

TOE 的低层设计提供了以模块和它们之间相互关系和依赖关系的观点，描述了 TSF 的内部工作方式。低层设计还保证了正确有效地细化子 TSF 子系统。

对于 TSF 的每一个模块，低层设计描述了它的用途、功能、接口、依赖关系和所有 TSP-实施功能的实现。

组件分级：

本子类的组件分级，是基于低层设计所要求的形式化程度和接口规范所要求的详细程度。

应用注释：

术语“TSP-实施模块”是指正确实施 TSP 所必须依赖的任意模块。

术语“安全功能性”用来表示针对由 TOE 实现的一些安全功能，一个模块所执行的一系列操作。这种差别产生的原因是模块不必与特定的安全功能相关。一个给定的模块可能直接对应于一个或若干个安全功能，也可能是许多模块必须结合在一起才能实现一个单一的安全功能。

ADV _ LLD. *. 6C 元素要求低层设计应描述每一个 TSP 实施功能是如何提供的。这个要求旨在希望低层设计能提供一个预见每个模块如何实现设计意图的描述。

本子类的 ADV _ LLD. *. 2E 元素定义了这样一个要求，即要求评估者判定低层设计是满足 TOE 安全功能要求的一个精确且完备的实例化。这就提供了低层设计和 TOE 安全功能要求之间的一种直接对应性，以作为 ADV _ RCR 子类所要求的成对对应性的补充。我们希望评估者利用 ADV _ RCR 中提供的证据作为该判定的输入，将对完备性的要求与低层设计的抽象程度联系起来。

ADV _ LLD. 2. 9C 引入了一个完备地表示模块接口的要求。这将为支持 TOE 彻底测试(利用 ATE _ DPT 组件)和脆弱性评定提供必要的细节。

在低层设计的形式化程度的上下文中，非形式化、半形式化和形式化三个等级的的划分实际上都是主观的。因此，ADV _ LLD. 1. 1C 也能够满足半形式化或者形式化的低层设计。此外，ADV _ LLD. 2. 1C 也能够满足形式化的低层设计。

ADV _ LLD. 1　描述性低层设计

依赖关系：

ADV _ HLD. 2　安全加强的高层设计

ADV _ RCR. 1　非形式化对应性论证

开发者行为元素：

ADV _ LLD. 1. 1D 开发者应当提供 TSF 的低层设计。

证据的内容和形式元素：

ADV _ LLD. 1. 1C　低层设计的表示应当是非形式化的。

ADV _ LLD. 1. 2C　低层设计应当是内在一致的。

ADV _ LLD. 1. 3C　低层设计应当以模块方式来描述 TSF。

ADV _ LLD. 1. 4C　低层设计应当描述每一个模块的用途。

ADV _ LLD. 1. 5C　低层设计应当依据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系。

ADV _ LLD. 1. 6C　低层设计应当描述每一个 TSP 实施功能是如何被提供的。

ADV _ LLD. 1. 7C　低层设计应当标识 TSF 模块的所有接口。

ADV _ LLD. 1. 8C　低层设计应当标识 TSF 模块的哪些接口是外部可见的。

ADV _ LLD. 1. 9C　低层设计应当描述 TSF 模块所有接口的用途和用法，适当时，应提供影响、例外情况和错误消息的细节。

ADV _ LLD. 1. 10C　低层设计应当描述如何将 TOE 分离成 TSP 实施模块和其他模块。

评估者行为元素：

ADV _ LLD. 1. 1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ LLD. 1. 2E　评估者应当决定低层设计是 TOE 安全功能要求的一个精确且完备的实例化。

ADV _ LLD. 2　半形式化低层设计

依赖关系：

ADV_HLD.3 半形式化高层设计

ADV_RCR.2 半形式化对应性论证

开发者行为元素：

ADV_LLD.2.1D 开发者应当提供 TSF 的低层设计。

证据的内容和形式元素：

ADV_LLD.2.1C 低层设计的表示应当是**半形式化**的。

ADV_LLD.2.2C 低层设计应当是内在一致的。

ADV_LLD.2.3C 低层设计应当以模块方式来描述 TSF。

ADV_LLD.2.4C 低层设计应当描述每一个模块的用途。

ADV_LLD.2.5C 低层设计应当依据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系。

ADV_LLD.2.6C 低层设计应当描述每一个 TSP 实施功能是如何被提供的。

ADV_LLD.2.7C 低层设计应当标识 TSF 模块的所有接口。

ADV_LLD.2.8C 低层设计应当标识 TSF 模块的哪些接口是外部可见的。

ADV_LLD.2.9C 低层设计应当描述 TSF 模块所有接口的用途和用法，适当时，应提供**所有**影响、例外情况和错误消息的**全部**细节。

ADV_LLD.2.10C 低层设计应当描述如何将 TOE 分离成 TSP 实施模块和其他模块。

评估者行为元素：

ADV_LLD.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV_LLD.2.2E 评估者应当决定低层设计是 TOE 安全功能要求的一个精确且完备的实例化。

ADV_LLD.3 形式化低层设计

依赖关系：

ADV_HLD.5 形式化高层设计

ADV_RCR.3 形式化对应性论证

开发者行为元素：

ADV_LLD.3.1D 开发者应提供 TSF 的低层设计。

证据的内容和形式元素：

ADV_LLD.3.1C 低层设计的表示应当是**形式化**的。

ADV_LLD.3.2C 低层设计应当是内在一致的。

ADV_LLD.3.3C 低层设计应当以模块方式来描述 TSF。

ADV_LLD.3.4C 低层设计应当描述每一个模块的用途。

ADV_LLD.3.5C 低层设计应当依据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系。

ADV_LLD.3.6C 低层设计应当描述每一个 TSP 实施功能是如何被提供的。

ADV_LLD.3.7C 低层设计应当标识 TSF 模块的所有接口。

ADV_LLD.3.8C 低层设计应当标识 TSF 模块的哪些接口是外部可见的。

ADV_LLD.3.9C 低层设计应当描述 TSF 模块所有接口的用途和用法，适当时，应提供所有影响、例外情况和错误消息的全部细节。

ADV_LLD.3.10C 低层设计应当描述如何将 TOE 分离成 TSP 加强模块和其他模块。

评估者行为元素：

ADV_LLD.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _LLD.3.2E　评估者应当决定低层设计是 TOE 安全功能要求的一个精确而完备的实例化。

11.6　表示对应性(ADV _RCR)

目的：

各种 TSF 表示(如 TOE 概要规范、功能规范、高层设计、低层设计、实现表示)之间的对应性是所提供的最不抽象的 TSF 表示要求的一个精确且完备的实例化。这个结论是通过对所有相邻表示抽象之间的对应性判定结果逐步细化并累加而得出的。

组件分级：

本子类的组件分级，基于各种 TSF 表示之间的对应性所需的形式化程度。

应用注释：

开发者必须为评估者论证，所提供的最详尽的或最不抽象的 TSF 表示是功能表述的一个精确的、一致的、且完备的实例化，该功能就是 ST 中所表示的功能要求。通过说明相邻表示之间在相应严格程度上的对应性，来实现上述的要求。

该子类的要求不是旨在表述与 TSP 模型或 TSP 本身有关的对应性。而是如图 10.2 所示，它旨在表述所提供的各种 TSF 表示(如 TOE 概要规范、功能规范、高层设计、低层设计、实现表示)间的对应性。

ADV _RCR.*.1C 元素在定义 TSF 表示的邻对之间细化一些什么的范围时，提到“所有相关的安全功能”。对于 TOE 概要规范和功能规范之间的细化，本元素仅仅要求在 TOE 概要规范中的 TOE 安全功能在功能规范中进行细化，而不要求功能规范包含任何有关保证措施的细节(该细节将在 TOE 概要规范中提出)。当仅仅为一个 TSF 子集提供实现表示时(就象在 ADV _IMP.1 中)，低层设计和实现表示之间所要求的细化则被限制于实现表示所提出的安全功能之内。在所有其他情况下，本元素要求较为抽象的 TSF 表示的所有部分在较不抽象的 TSF 表示中进行细化。

在相邻 TSF 表示间对应性的形式化程度的上下文中，非形式化、半形式化和形式化三个等级的划分实际上都是主观的。因此，ADV _RCR.2.2C 和 ADV _RCR.3.2C 可能满足对应性形式化的证明。并且在缺乏形式化程度的任何要求时，对应性的论证可以是非形式化的、半形式化的或者形式化的。

ADV _RCR.1　非形式化对应性论证

依赖关系：

无依赖关系。

开发者行为元素：

ADV _RCR.1.1D　开发者应当在所提供的 TSF 表示的所有相邻对之间提供其对应性分析。

证据的内容和形式元素：

ADV _RCR.1.1C　对于所提供的 TSF 表示的每个相邻对，分析应当论证，较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

评估者行为元素：

ADV _RCR.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _RCR.2　半形式化对应性论证

依赖关系：

无依赖关系。

开发者行为元素：

ADV _ RCR. 2. 1D 开发者应当在所提供的 TSF 表示的所有相邻对之间提供其对应性分析。

证据的内容和形式元素：

ADV _ RCR. 2. 1C 对于所提供的 TSF 表示的每个相邻对，分析应当论证，较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

ADV _ RCR. 2. 2C 对于所提供的 TSF 表示的每个相邻对，两者的各部分都至少是以半形式化来规定时，表示部分之间的对应性论证也应当是半形式化的。

评估者行为元素：

ADV _ RCR. 2. 1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ RCR. 3 形式化对应性论证

应用注释：

开发者必须论证或严格证明对应性，像以下的要求所描述的那样，该对应性是论证还是严格证明应当与表示风格的严格程度相称。例如，当相应的表示是形式化规定的时候，对应性必须是严格证明。

依赖关系：

无依赖关系。

开发者行为元素：

ADV _ RCR. 3. 1D 开发者应当在所提供的 TSF 表示的所有相邻对之间提供其对应性分析。

ADV _ RCR. 3. 2D 对于那些形式化规定的表示的相应部分，开发者应当严格证明其对应性。

证据的内容和形式元素：

ADV _ RCR. 3. 1C 对于所提供的 TSF 表示的每个相邻对，分析应当严格证明或论证，较为抽象的 TSF 表示的所有相关安全功能性都在较不抽象的 TSF 表示中得到正确、完整的细化。

ADV _ RCR. 3. 2C 对于所提供的 TSF 表示的每个相邻对，当其中**一个表示的某些部分是半形式化规定的，而另一个表示的对应部分**至少是半形式化规定时，表示部分之间的对应性论证也应当是半形式化的。

ADV _ RCR. 3. 3C 对于所提供的 TSF 表示的每个相邻对，两者的各部分都是形式化规定的，表示部分之间的对应性的证明也应当是形式化的。

评估者行为元素：

ADV _ RCR. 3. 1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ RCR. 3. 2E **评估者应当通过选择性地验证那些形式化分析来决定对应性证明的准确性。**

11.7 安全策略模型(ADV _ SPM)

目的：

这一个子类目的是提供额外的保证，即在功能规范中的安全功能可以实施 TSP 中的策略。它的实现，是通过开发一个基于 TSP 策略子集的安全策略模型，并确定功能规范、安全策略模型和 TSP 策略之间的对应性。

组件分级：

本子类的组件分级，是基于 TSP 模型所要求的形式化的程度，以及 TSP 模型和功能规范之间对应性所要求的形式化的程度。

应用注释：

TSP 可以包括任何策略，而 TSP 模型仅仅表示了这些策略的某些子集，因为对特定的策略进行模

型化已超越了当前的技术水平。但当前的技术水平可以确定部分策略可模型化，因此 PP/ST 作者标识出一些特定的功能，和可以(于是要求)进行模型化的相关策略。至少，访问控制和信息流控策略是要求进行模型化的(如果它们是 TSP 的部分)，因为这两者处于当前技术水平之内。

对于本子类中的每个组件，要求描述 TSP 模型中 TSP 应用策略的规则和特征，并且确保 TSP 模型满足 TSP 的相应策略。TSP 模型的“规则”和“特征”是为了引进可开发模型类型的灵活性(如状态转换，无干扰)。例如，规则可能表示为“属性”(如简单安全属性)，特征可能表示为一些定义，诸如“初始状态”、“安全状态”、“主体”和“客体”。

在 TSP 模型和 TSP 模型及功能规范之间的对应性的形式化程度的上下文中，非形式化、半形式化和形式化三个等级的的划分实际上都是主观的。因此，ADV _ SPM. 1. 1C 也可以满足半形式化或者形式化的 TSP 模型，而 ADV _ SPM. 2. 1C 可以满足形式化的 TSP 模型。进而，ADV _ SPM. 2. 5C 和 ADV _ SPM. 3. 5C 可满足对应性的形式化证明。最后，在缺乏形式化程度的任何要求时，对应性的论证可以是非形式化的、半形式化的或者形式化的。

ADV _ SPM. 1　非形式化 TOE 安全策略模型

依赖关系：

ADV _ FSP. 1 非形式化功能规范

开发者行为元素：

ADV _ SPM. 1. 1D　开发者应提供一个 TSP 模型。

ADV _ SPM. 1. 2D　开发者应论证功能规范和 TSP 模型之间的对应性。

证据的内容和形式元素：

ADV _ SPM. 1. 1C　TSP 模型应当是非形式化的。

ADV _ SPM. 1. 2C　TSP 模型应当描述所有可以模型化的 TSP 策略的规则与特征。

ADV _ SPM. 1. 3C　TSP 模型应当包括一个基本原理，即论证该模型对于所有可模型化的 TSP 策略来说，是与其一致的，而且是完备的。

ADV _ SPM. 1. 4C　TSP 模型和功能规范之间的对应性论证应当说明，所有功能规范中的安全功能对于 TSP 模型来说，是与其一致，而且是完备的。

评估者行为元素：

ADV _ SPM. 1. 1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ SPM. 2　半形式化 TOE 安全策略模型

依赖关系：

ADV _ FSP. 1 非形式化功能规范

开发者行为元素：

ADV _ SPM. 2. 1D　开发者应提供一个 TSP 模型。

ADV _ SPM. 2. 2D　开发者应论证功能规范和 TSP 模型之间的对应性。

证据的内容和形式元素：

ADV _ SPM. 2. 1C　TSP 模型应当是半形式化的。

ADV _ SPM. 2. 2C　TSP 模型应当描述所有可以模型化的 TSP 策略的规则与特征。

ADV _ SPM. 2. 3C　TSP 模型应当包括一个基本原理，即论证该模型对于所有可模型化的 TSP 策略来说，是与其一致的，而且是完备的。

ADV _ SPM. 2. 4C　TSP 模型和功能规范之间的对应性论证应当说明，所有功能规范中的安全功能对于 TSP 模型来说，是与其一致，而且是完备的。

ADV _ SPM. 2. 5C　功能规范至少是半形式化时，TSP 模型与功能规范之间的对应性的论证也应是半形式化的。

评估者行为元素：

ADV _ SPM.2.1E　评估者将确认所提供的信息满足证据的内容和形式的所有要求。

ADV _ SPM.3　形式化 TOE 安全策略模型

依赖关系：

ADV _ FSP.1 非形式化功能规范

开发者行为元素：

ADV _ SPM.3.1D　开发者应提供一个 TSP 模型。

ADV _ SPM.3.2D　开发者应论证**或适当时严格证明**功能规范和 TSP 模型之间的对应性。

证据的内容和形式元素：

ADV _ SPM.3.1C　TSP 模型应当是**形式化的**。

ADV _ SPM.3.2C　TSP 模型应当描述所有可以模型化的 TSP 策略的规则与特征。

ADV _ SPM.3.3C　TSP 模型应当包括一个基本原理，即论证该模型对于所有可模型化的 TSP 策略来说，是与其一致的，而且是完备的。

ADV _ SPM.3.4C　TSP 模型和功能规范之间的对应性论证应当说明，所有功能规范中的安全功能对于 TSP 模型来说，是与其一致，而且是完备的。

ADV _ SPM.3.5C　功能规范是**半形式化时**，TSP 模型与功能规范之间的对应性论证应当是半形式化的。

ADV _ SPM.3.6C　功能规范是形式化时，TSP 模型与功能规范之间的对应性证明应当是形式化的。

评估者行为元素：

ADV _ SPM.1.1E　评估者将确认所提供的信息满足证据的内容和形式的所有要求。

12　AGD 类：指导性文档

指导性文档类提供了关于用户和管理员指南的要求。为了安全地管理和使用 TOE，该类有必要描述所有有关 TOE 安全应用方面的内容。

图 12.1 给出了本类中的子类以及子类中的各组件之间的层次关系。

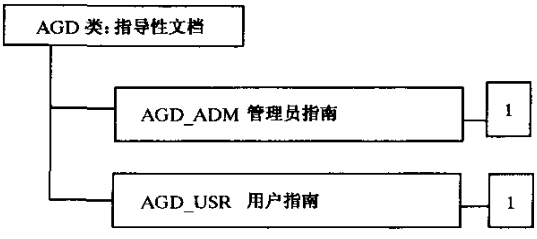

图 12.1　指导性文档类分解

12.1　管理员指南(AGD _ ADM)

目的：

管理员指南是指一种书面材料，其目的是让负责设置、维护和管理 TOE 的人以正确的方式，最大限度地保证安全。由于 TOE 的安全运行依赖于 TSF 的正确执行，所以负责完成这些功能的人必须是 TSF 所信任的。管理员指南将帮助管理员理解 TOE 提供的安全功能，这些功能包括要求管理员采取紧急安全措施和提供紧急安全信息。

组件分级：

本子类仅包含一个组件。

应用注释：

在管理员指南中都适当地包含了以下的要求：即 AGD _ ADM.1.3C 和 AGD _ ADM.1.7C 应包括对 TOE 用户有关 TOE 安全环境的任何警告，以及 PP/ST 中描述的安全目标。

AGD _ ADM.1.5C 中所提及的安全价值的概念与管理员控制安全的参数有关。我们有必要对安全和不安全地设置这些参数提供指南。这个概念与 GB/T 18336 第 2 部分中组件 FMT _ MSA.2 的使用有关。

AGD _ ADM.1　管理员指南

依赖关系：

ADV _ FSP.1 非形式化功能规范

开发者行为元素：

AGD _ ADM.1.1D 开发者应当提供针对系统管理员的管理员指南。

证据的内容和形式元素：

AGD _ ADM.1.1C　管理员指南应当描述 TOE 管理员可使用的管理功能和接口。

AGD _ ADM.1.2C　管理员指南应当描述如何以安全的方式管理 TOE。

AGD _ ADM.1.3C　管理员指南应当包含在安全处理环境中必须进行控制的功能和权限的警告。

AGD _ ADM.1.4C　管理员指南应当描述所有与 TOE 的安全运行有关的用户行为的假设。

AGD _ ADM.1.5C　管理员指南应当描述所有受管理员控制的安全参数，合适时，应指明安全值。

AGD _ ADM.1.6C　管理员指南应当描述每一种与需要执行的管理功能有关的安全相关事件，包括改变 TSF 所控制的实体的安全特性。

AGD _ ADM.1.7C　管理员指南应当与为评估而提供的其他所有文档保持一致。

AGD _ ADM.1.8C　管理员指南应当描述与管理员有关的 IT 环境的所有安全要求。

评估行为元素：

AGD _ ADM.1.1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

12.2　用户指南(AGD _ USR)

目的：

用户指南指 TOE 的非管理员类用户或其他使用 TOE 外部接口的人员(如，程序员)所使用的材料。用户指南描述 TSF 提供的安全功能，安全使用的指令和指导方针，包括警报。

用户指南提供了关于 TOE 使用和可信度的测量的假设基础，这样非恶意的用户、应用提供者和其他使用 TOE 外部接口的人员都能理解 TOE 安全运行并自觉执行。

组件分级：

本子类仅包含一个组件。

应用注释：

在用户指南中都适当地包含了以下的要求：即 AGD _ USR.1.3.C 和 AGD _ USR.1.5C 应包括对 TOE 用户有关 TOE 安全环境的任何警告，以及 PP/ST 中描述的安全目标。

在许多情况之下，指南可以适当地以单独文档的形式提出：一份要提供给一般用户，一份要提供给使用软硬件接口的应用程序员或硬件设计员。

AGD _ USR.1　用户指南

依赖关系：

ADV _ FSP.1　非形式化功能规范

开发者行为元素：

AGD _ USR. 1. 1D　开发者应当提供用户指南。

证据的内容和形式元素：

AGD _ USR. 1. 1C　用户指南应该描述 TOE 的非管理员用户可用的功能和接口。

AGD _ USR. 1. 2C　用户指南应该描述 TOE 提供的用户可访问的安全功能的用法。

AGD _ USR. 1. 3C　用户指南应该包含受安全处理环境中所控制的用户可访问的功能和权限的警告。

AGD _ USR. 1. 4C　用户指南应该清晰地阐述 TOE 安全运行中用户所必须负的职责，包括有关在 TOE 安全环境阐述中找得到的用户行为的假设。

AGD _ USR. 1. 5C　用户指南应该与为评估而提供的其他所有文档保持一致。

AGD _ USR. 1. 6C　用户指南应该描述与用户有关的 IT 环境的所有安全要求。

评估者行为元素：

AGD _ USR. 1. 1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

13　ALC 类：生命周期支持

生命周期支持是在 TOE 开发和维护阶段，对其进行细化而建立原则和控制。如果安全分析和证据产生作为开发和维护活动的完整部分在常规的基础上进行，那么 TOE 和它的安全要求之间对应性的信任度将得到加强。

图 13.1 给出本类中的子类，以及子类中的各组件之间的层次关系。

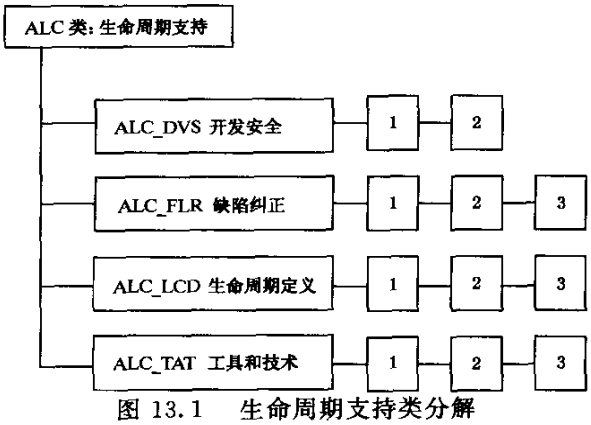

图 13.1　生命周期支持类分解

13.1　开发安全(ALC _ DVS)

目的：

开发安全涉及到了为保护 TOE 而在开发环境中采用的物理、程序、人员以及其他方面的安全措施。它包括开发场地的物理安全和开发人员的选择程序。

组件分级：

本子类的组件分级，是基于所要求的安全措施的充分性是否需要证明。

应用注释：

本子类涉及到去除或降低开发场地所面临的威胁的措施。相反地，TOE 用户场地所要对抗的威胁通常存在于 PP 或 ST 的安全环境中。

评估者应该决定是否有必要去参观开发场地以确认本子类的要求得到了满足。

应该意识到，保密性在 TOE 的开发环境中对 TOE 的保护并不总是问题，“必要的”一词的使用，是

考虑要选择适当的防护措施。

ALC_DVS.1 安全措施标识

依赖关系：

无依赖关系。

开发者行为元素：

ALC_DVS.1.1D **开发者应提供开发安全文档。**

证据的内容和形式元素：

ALC_DVS.1.1C **开发安全文档应描述在 TOE 的开发环境中，用以保护 TOE 设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施。**

ALC_DVS.1.2C **开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。**

评估者行为元素：

ALC_DVS.1.1E **评估者应确认所提供的信息满足证据的内容和形式的所有要求。**

ALC_DVS.1.2E **评估者应确认应用了安全措施。**

ALC_DVS.2 安全措施的充分性

依赖关系：

无依赖关系。

开发者行为元素：

ALC_DVS.2.1D 开发者应提供开发安全文档。

证据的内容和形式元素：

ALC_DVS.2.1C 开发安全文档应描述在 TOE 的开发环境中，用以保护 TOE 设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施。

ALC_DVS.2.2C 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。

ALC_DVS.2.3C **证据应能证明安全措施对维护 TOE 的保密性和完整性提供了必要的保护级别。**

评估者行为元素：

ALC_DVS.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_DVS.2.2E 评估者应确认应用了安全措施。

13.2 缺陷纠正(ALC_FLR)

目的：

缺陷纠正要求开发者对已发现的安全缺陷进行跟踪和纠正。虽然评估 TOE 时无法确定将来缺陷纠正过程中的一致性，但可以评估开发者跟踪和纠正缺陷，以及发布缺陷信息和更正所采取的策略和过程。

组件分级：

本子类的组件分级，是基于缺陷纠正程序的范围的不断扩大和缺陷纠正策略的严格性程度不断加深。

应用注释：

本子类保证将来对 TOE 进行维护和支持，它要求 TOE 的开发者跟踪和纠正 TOE 的缺陷。除此以外，还要求发布缺陷的纠正。该子类并不在目前的评估水平上强加评估要求。

缺陷纠正程序应当描述遇到所有缺陷时的处理方法。当缺陷不能被修复和采取其他的措施(例如程

序措施)的情况也存在。所提供的文档应当包括以下的程序:为操作方提供缺陷修复,当缺陷修复延时(在过渡期间应采取的措施)或缺陷已不可能修补时,应提供缺陷信息。

ALC_FLR.1 基本缺陷纠正

依赖关系:

无依赖关系。

开发者行为元素:

ALC_FLR.1.1D **开发者应将缺陷纠正的程序文档化。**

证据的内容和形式元素:

ALC_FLR.1.1C **缺陷纠正程序文档应描述用以跟踪所有在 TOE 发布时已被报道的安全缺陷的程序。**

ALC_FLR.1.2C **缺陷纠正程序应当要求描述所提供的每个安全缺陷的性质和效果,以及更正缺陷的情况。**

ALC_FLR.1.3C **缺陷纠正程序应当要求标识每个安全缺陷所采取的纠正措施。**

ALC_FLR.1.4C **缺陷纠正程序文档应当描述为 TOE 用户的更正行为所提供的信息、更正和指导的方法。**

评估者行为元素:

ALC_FLR.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_FLR.2 缺陷报告过程

依赖关系:

无依赖关系。

开发者行为元素:

ALC_FLR.2.1D 开发者应将缺陷纠正的程序文档化。

ALC_FLR.2.2D **开发者应建立一个程序来接受用户对于安全缺陷的报告和更正这些缺陷的要求,并采取相应的解决措施。**

证据的内容和形式元素:

ALC_FLR.2.1C 缺陷纠正程序文档应描述用以跟踪所有在 TOE 发布时已被报道的安全缺陷的程序。

ALC_FLR.2.2C 缺陷纠正程序应当要求描述所提供的每个安全缺陷的性质和效果,以及更正缺陷的情况。

ALC_FLR.2.3C 缺陷纠正程序应当要求标识每个安全缺陷所采取的更正措施。

ALC_FLR.2.4C 缺陷纠正程序文档应当描述为 TOE 用户的更正行为所提供的信息、更正和指导的方法。

ALC_FLR.2.5C **处理已报道的安全缺陷的程序必须确保所有已知缺陷都已被更正,并且更正办法发布给 TOE 用户。**

ALC_FLR.2.6C 处理已报道的安全缺陷的程序必须提供防范机制,确保为更正这些安全缺陷所引进的更正方法不会带来新的缺陷。

评估者行为元素:

ALC_FLR.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_FLR.3 系统缺陷纠正

依赖关系:

无依赖关系。

开发者行为元素：

ALC _ FLR. 3. 1D 开发者应将缺陷纠正的程序文档化。

ALC _ FLR. 3. 2D 开发者应建立一个程序来接受用户对于安全缺陷的报告和更正这些缺陷的要求，并采取相应的解决措施。

ALC _ FLR. 3. 3D **开发者应为用户有关 TOE 的安全问题的报告和查询指明一个或多个的特别联系点。**

证据的内容和形式元素：

ALC _ FLR. 3. 1C 缺陷纠正程序文档应描述用以跟踪所有在 TOE 发布时已被报道的安全缺陷的程序。

ALC _ FLR. 3. 2C 缺陷纠正程序应当要求描述所提供的每个安全缺陷的性质和效果，以及更正缺陷的情况。

ALC _ FLR. 3. 3C 缺陷纠正程序应当要求标识每个安全缺陷所采取的更正措施。

ALC _ FLR. 3. 4C 缺陷纠正程序文档应当描述为 TOE 用户的更正行为所提供的信息、更正和指导的方法。

ALC _ FLR. 3. 5C 处理已报道的安全缺陷的程序必须确保所有已知缺陷都已被更正，并且更正办法发布给 TOE 用户。

ALC _ FLR. 3. 6C 处理已报道的安全缺陷的程序必须提供防范机制，确保为更正这些安全缺陷所引进的更正方法不会带来新的缺陷。

ALC _ FLR. 3. 7C **缺陷纠正程序应包括这样一个程序，它负责及时将安全缺陷报告及其相应的更正自动交付给可能受到这安全缺陷影响的注册用户。**

评估者行为元素：

ALC _ FLR. 3. 1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

13.3 生命周期定义(ALC _ LCD)

目的：

TOE 的开发和维护缺乏控制将导致有缺陷的 TOE 实现（或者导致 TOE 不满足其所有的安全要求），这便违背了安全性原则。因此，尽早在 TOE 生命周期内建立 TOE 开发和维护的模型是很重要的。

使用 TOE 开发和维护的模型并不能确保 TOE 不会有缺陷，也不能确保 TOE 能满足它所有的安全功能要求。选择的模型不充分或不恰当，将无助于提高 TOE 的质量。使用一个由专家组（例如学科专家、标准化实体）提出的生命周期模型，将会有利于开发和维护模型，提高 TOE 的整体质量。

组件分级：

本子类的组件分级，是基于对生命周期模型的标准化、可测性，以及对其一致性不断提高的要求。

应用注释：

生命周期模型包括用于开发和维护 TOE 的程序、工具和技术。这个模型所涉及的过程包括设计方法、评审程序、项目管理控制、转换控制程序、测试方法和接收程序。一个有效的生命周期模型在整个职责分配和进程监控的管理结构中，将表明开发和维护过程的以上方面。

虽然生命周期定义涉及的是 TOE 的维护，因而同时涉及评估完成后的相关方面，但它通过对评估时所提供的 TOE 生命周期信息加以分析，从而增加了评估的保证。

一个标准的生命周期模型是为某些专家组所认可的模型（例如学科专家、标准化实体）。

一个可测量的生命周期模型是带有算术参数或测量 TOE 开发特性的量度（例如源码复杂性量

度)。

如果开发者能够提供信息,证明一个生命周期模型适当地减少了安全威胁的危险性,那么该生命周期模型就为 TOE 的开发和维护提供了必要的控制。ST 中提供的有关 TOE 预期的环境和 TOE 的安全目的的信息,在定义生命周期模型中 TOE 交付之后的一部分是有用的。

ALC_LCD.1 开发者定义的生命周期模型

依赖关系:

无依赖关系。

开发者行为元素:

ALC_LCD.1.1D **开发者应建立生命周期模型用于开发和维护 TOE。**

ALC_LCD.1.2D **开发者应提供生命周期定义文档。**

证据的内容和形式元素:

ALC_LCD.1.1C **生命周期定义文档应描述用于开发和维护 TOE 的模型。**

ALC_LCD.1.2C **生命周期模型应提供对 TOE 开发和维护所必要的控制。**

评估者行为元素:

ALC_LCD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_LCD.2 标准化生命周期模型

依赖关系:

无依赖关系。

开发者行为元素:

ALC_LCD.2.1D 开发者应建立生命周期模型用于开发和维护 TOE。

ALC_LCD.2.2D 开发者应提供生命周期定义文档。

ALC_LCD.2.3D 开发者应利用标准化的生命周期模型来开发和维护 TOE。

证据的内容和形式元素:

ALC_LCD.2.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型。

ALC_LCD.2.2C 生命周期模型应提供对 TOE 开发和维护所必要的控制。

ALC_LCD.2.3C 生命周期定义文档应解释选择该模型的原因。

ALC_LCD.2.4C 生命周期定义文档应解释如何用该模型来开发和维护 TOE。

ALC_LCD.2.5C 生命周期定义文档应论证与标准化的生命周期模型的一致性。

评估者行为元素:

ALC_LCD.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_LCD.3 可测量的生命周期模型

依赖关系:

无依赖关系。

开发者行为元素:

ALC_LCD.3.1D 开发者应建立生命周期模型用于开发和维护 TOE。

ALC_LCD.3.2D 开发者应提供生命周期定义文档。

ALC_LCD.3.3D 开发者应利用标准化的**可测量的**生命周期模型来开发和维护 TOE。

ALC_LCD.3.4D 开发者应利用标准化的和可测量的生命周期模型来衡量 TOE 的开发。

证据的内容和形式元素:

ALC_LCD.3.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型,**包括针对该模型衡量 TOE**

开发所需的算术参数或量度的细节。

ALC _ LCD.3.2C 生命周期模型应提供对 TOE 开发和维护所必要的控制。

ALC _ LCD.3.3C 生命周期定义文档应解释选择该模型的原因。

ALC _ LCD.3.4C 生命周期定义文档应解释如何用该模型来开发和维护 TOE。

ALC _ LCD.3.5C 生命周期定义文档应论证与标准化的可测量的生命周期模型的一致性。

ALC _ LCD.3.6C 生命周期文档应利用标准化的可测量的生命周期模型，来提供 TOE 开发的测量结果。

评估者行为元素：

ALC _ LCD.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

13.4 工具和技术(ALC _ TAT)

目的：

工具和技术是选择用于开发、分析和实现 TOE 的工具的一个方面。它包括防止用定义含糊、不一致或不正确的开发工具来开发 TOE 的要求。这包括编程语言、文档、实现标准以及其他的诸如支持运行的程序库的 TOE 部分，但又不限于以上所说的。

组件分级：

本子类的组件分级，是基于在实现标准及其选项文档的描述和范围上增加的要求。

应用注释：

对明确定义的开发工具有一定的要求。这些工具已证明无需进一步检验就可应用。例如，基于标准实体公开发布的程序语言和计算机辅助设计系统(CAD)标准，它们是明确定义的。

工具和技术的区别在于开发者使用的实现标准(ALC _ TAT.2.3D)和“TOE 的所有部分”的实现标准(ALT _ TAT.3.3D)的不同，另外还包括第三方的软件、硬件或固件的不同。

ALC _ TAT.1.2C 中的要求尤其适用于程序语言，以便确保所有源代码里的语句都有其明确的含义。

ALC _ TAT.1 明确定义的开发工具

依赖关系：

ADV _ IMP.1 TSF 实现的子集

开发者行为元素：

ALC _ TAT.1.1D **开发者应标识用于开发 TOE 的工具。**

ALC _ TAT.1.2D **开发者应文档化已选择的依赖实现的开发工具的选项。**

证据的内容和形式元素：

ALC _ TAT.1.1C **所有用于实现的开发工具都必须有明确定义。**

ALC _ TAT.1.2C **开发工具文档应无歧义地定义实现中每个语句的含义。**

ALC _ TAT 1.3C **开发工具文档应无歧义地定义所有基于实现的选项的含义。**

评估者行为元素：

ALC _ TAT.1.1E **评估者应确认所提供的信息满足证据的内容和形式的所有要求。**

ALC _ TAT.2 遵从实现标准

依赖关系：

ADV _ IMP.1 TSF 实现的子集

开发者行为元素：

ALC _ TAT. 2. 1D　开发者应标识用于开发 TOE 的工具。

ALC _ TAT. 2. 2D　开发者应文档化已选择的依赖实现的开发工具的选项。

ALC _ TAT. 2. 3D　开发者应描述所应用的实现标准。

证据的内容和形式元素：

ALC _ TAT. 2. 1C　所有用于实现的开发工具都必须有明确定义。

ALC _ TAT. 2. 2C　开发工具文档应无歧义地定义实现中每个语句的含义。

ALC _ TAT 2. 3C　开发工具文档应无歧义地定义所有基于实现的选项的含义。

评估者行为元素：

ALC _ TAT. 2. 1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC _ TAT. 2. 2E　**评估者应确认实现标准被采用。**

ALC _ TAT. 3　遵从实现标准——所有部分

依赖关系：

ADV _ IMP. 1　TSF 实现的子集

开发者行为元素：

ALC _ TAT. 3. 1D　开发者应标识用于开发 TOE 的工具。

ALC _ TAT. 3. 2D　开发者应文档化已选择的依赖实现的开发工具的选项。

ALC _ TAT. 3. 3D　开发者应描述所应用的 **TOE 所有部分的**实现标准。

证据的内容和形式元素：

ALC _ TAT. 3. 1C　所有用于实现的开发工具都必须有明确定义。

ALC _ TAT. 3. 2C　开发工具文档应无歧义地定义实现中每个语句的含义。

ALC _ TAT 3. 3C　开发工具文档应无歧义地定义所有基于实现的选项的含义。

评估者行为元素：

ALC _ TAT. 3. 1E　评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC _ TAT. 3. 2E　评估者应确认实现标准被采用。

14　ATE 类：测试

“测试”类包括四个子类：覆盖范围(ATE _ COV)、深度(ATE _ DPT)、独立性测试(例如由评估者执行的功能测试)(ATE _ IND)和功能测试(ATE _ FUN)。测试有助于确保 TOE 满足其安全功能的要求。测试提供这样的保证：TOE 至少满足 TOE 的安全功能要求，但是不能确定 TOE 是否仅做了规定的事情。测试还可以直接面向 TSF 的内部结构，诸如根据规范对各个子系统和模块进行测试。

为了增强应用该子类组件的灵活性，覆盖范围和深度测试应与功能测试分离。然而，这三个子类中的要求又往往需要一起应用。

独立性测试子类依赖于别的子类提供必要的信息来支持其要求，但主要与独立评估者的行为有关。

本类的重点在于确保 TSF 根据规范进行运作。这将包括两种测试：基于功能要求的正面测试和检测不良行为是否不存在的反面测试。本类不说明穿透性测试，即直接寻找用户违反安全策略的脆弱性。穿透性测试是基于 TOE 的分析，它在 TSP 设计和实现中特意寻找并确定其脆弱性。这在 AVA 类中作为脆弱性评估的一个方面单独地进行说明。

图 14.1　给出本类中的子类，以及子类中的组件层次。

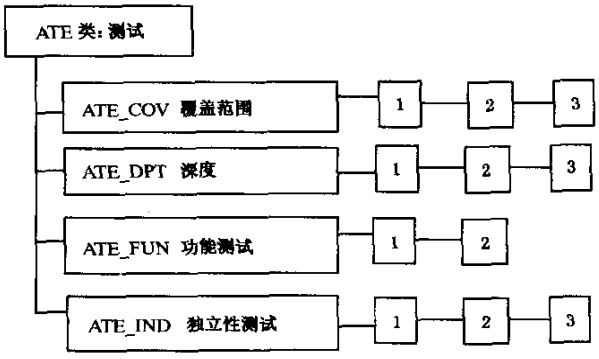

图 14.1　测试类分解

14.1　覆盖范围（ATE _ COV）

目的：

本子类指出了有关测试范围完备性方面的内容。也就是说，它说明 TSF 要被测试的广度，以及测试是否广泛得足以论证 TSF 如规定的那样运作。

组件分级：

本子类的组件分级，是基于接口测试渐增的严格性，以及测试的充分性分析渐增的严格性，该测试论证 TSF 是根据功能规范而进行运作。

ATE _ COV.1　范围证据

目的：

本组件的目的是确定 TSF 已经按照功能规范进行了测试。这是通过开发者对对应性证据的检查来完成。

应用注释：

当测试目的是要覆盖 TSF 时，除了从测试到功能规范的非形式化映射和测试数据本身之外，不需要提供任何东西来验证这个结论。

在这个组件中，要求开发者表明标识的测试如何像功能规范中所描述的那样与 TSF 相一致。这可用对应性陈述来实现，或许还可以使用一张表格来说明。这个信息要求支持评估者为这次评估准备的测试程序。在这个级别上，不需要开发者覆盖 TSF 的各个方面，但评估者有必要考虑这个领域的不足之处。

依赖关系：

ADV _ FSP.1　非形式化功能规范

ATE _ FUN.1　功能测试

开发者行为元素：

ATE _ COV.1.1D　开发者应当提供测试覆盖范围的证据。

证据的内容和形式元素：

ATE _ COV.1.1C　测试覆盖范围的证据应当论证测试文档中所标识的测试和功能规范中所描述的 TSF 之间的对应性。

评估者行为元素：

ATE _ COV.1.1E　评估者应当确认提供的信息满足证据的内容和形式的所有要求。

ATE _ COV.2　范围分析

目的：

本组件的目的是确定 TSF 已经以系统的方法针对功能规范进行了测试。这将通过检查开发者一致性分析来实现。

应用注释：

要求评估者论证已标识的测试包括了在功能规范中描述的所有安全功能的测试。这个分析不能仅仅表明测试和安全功能间的对应性，还应该为评估者提供足够的信息来判定这些功能是如何执行的。这个信息还可用于计划评估者附加的测试。虽然在这一级别上，开发者将论证功能规范中的每个功能都已经被测试过了，但是关于每个功能的测试详尽程度不必十分彻底。

依赖关系：

ADV _ FSP.1　非形式化功能规范

ATE _ FUN.1　功能测试

开发者行为元素：

ATE _ COV.2.1D　开发者将提供测试覆盖范围的分析。

证据的内容和形式元素：

ATE _ COV.1.1C　测试覆盖范围的分析应当论证测试文档中所标识的测试和功能规范中所描述的 TSF 之间的对应性。

ATE _ COV.2.2C　测试覆盖范围的分析应当论证功能规范中所描述 TSF 和测试文档所标识的测试之间的对应性是完备的。

评估者行为元素：

ATE _ COV.2.1E　评估者应当确认提供的信息满足证据的内容和形式的要求。

ATE _ COV.3　范围的严格分析

目的：

本组件的目的是建立 TSF 已经以系统的方法对功能规范进行了测试。这将通过开发者检查一致性分析的检测来实现。

应用注释：

要求开发者提供令人信服的论点说明所标识的测试包括了所有安全功能，并且对每个安全功能的测试是完备的。评估者几乎没有余地来设计额外的基于功能规范的 TSF 接口的功能测试，因为它们已被彻底地测试过了。尽管如此，评估者应该努力设计这种测试。

依赖关系：

ADV _ FSP.1　非形式化功能规范

ATE _ FUN.1　功能测试

开发者行为元素：

ATE _ COV.3.1D　开发者将提供测试覆盖范围的分析。

证据的内容和形式元素：

ATE _ COV.3.1C　测试覆盖范围的证据应当论证测试文档中所标识的测试和功能规范中所描述的 TSF 之间的对应性。

ATE _ COV.3.2C　测试覆盖范围的分析应当论证功能规范中所描述 TSF 和测试文档所标识的测试之间的对应性是完备的。

ATE _ COV.3.3C　测试范围的分析应当严格地论证功能规范所标识的 TSF 的所有外部接口已经被完备测试过了。

评估者行为元素：

ATE _ COV.3.1E　评估者应当确认提供的信息满足证据的内容和形式的要求。

14.2 深度（ATE _ DPT）

目的：

本子类的组件涉及 TSF 测试所能到达的详细程度。安全功能的测试基于从表示分析中引出信息的不断增加的深度。

本子类的目的是防止在 TOE 的开发中遗漏错误。此外，本子类的组件，特别是当测试与 TSF 内部结构的关系越紧密，就越容易发现任何插入的恶意代码。

执行特定内部接口的测试不仅能保证 TSF 展现所期望的外部安全行为，而且能保证这种行为是从正确运作的内部机制中产生的。

组件分级：

本子类的组件分级，基于 TSF 表示所提供的从高层设计到实现表示不断增加的细节。这个分级反映了 ADV 类所提出的 TSF 表示。

应用注释：

一般而言，文档和证据的特定数目和类型将取决于从 ATE _ FUN 中选取的组件。

对这个级别的功能规范的测试由 ATE _ COV 提出。

本子类采取了这样的原则：即测试的级别要适合于所寻求的保证的级别。当应用高级组件时，要求测试的结果应论证 TSF 的实现与它的设计相一致。例如，高层设计应该非常详细地描述每一个子系统和这些子系统间的接口。测试的证据必须表明子系统间的接口已被执行。这可以通过对 TSF 的内部接口的测试来完成，或者通过分别对子系统接口的测试来完成，也许还可以使用一个测试套件来实现上述测试。当一个内部接口的某些方面不能通过外部接口进行测试时，我们应该证明这些方面是不必测试的，或者该内部接口必须直接测试。在后一种情况下，为了能进行直接测试，高层设计必须充分详尽。当设计变得具体时，为了校验内部接口的正确运行，本子类中高级组件的内部接口随之变得可见。当应用这些组件时，只用 TSF 的外部接口来提供测试深度的充足证据是很困难的，通常必须进行模块测试。

ATE _ DPT.1 测试：高层设计

目的：

TSF 的子系统为该 TSF 的内部工作提供了一个高层描述。为了论证存在某种缺陷而在这个子系统级别上进行的测试确保已正确实现了该子系统。

应用注释：

我们期望开发者以“子系统”的观点来描述该 TSF 高层设计的测试。“子系统”这个术语用来表示把 TSF 分解成数目相对较少的几部分这一概念。

依赖关系：

ADV _ HLD.1 描述性高层设计

ATE _ FUN.1 功能测试

开发者行为元素：

ATE _ DPT.1.1D 开发者应当提供测试深度的分析。

证据的内容和形式元素：

ATE _ DPT.1.1C 深度分析应当论证测试文档中所标识的测试足以论证该 TSF 运行是和高层设计一致的。

评估者行为元素：

ATE _ DPT.1.1E 评估者应当确认提供的信息满足证据的内容和形式的要求。

ATE _ DPT.2　测试:低层设计

目的:

TSF 的子系统提供这个 TSF 内部工作的一个高层描述。为了论证存在某种缺陷而在这个子系统级别上进行的测试确保已正确实现了该子系统。TSF 的模块提供 TSF 内部工作的描述。为了论证存在某种缺陷而对这个级别的模块进行的测试确保已正确实现了这些 TSF 模块。

应用注释:

我们期望开发者用"子系统"术语来描述对该 TSF 高层设计的测试。"子系统"这个术语用来表示把 TSF 分解成数目项目较少的几部分这一概念。

我们期望开发者根据"模块"来描述对该 TSF 低层设计的测试。"模块"这个术语用来表示把 TSF 每个"子系统"分解成数目较少的几部分这一概念。

依赖关系:

ADV _ HLD.2　安全加强的高层设计

ADV _ LLD.1　描述性低层设计

ATE _ FUN.1　功能测试

开发者行为元素:

ATE _ DPT.2.1D　开发者应当提供测试深度的分析。

证据的内容和形式元素:

ATE _ DPT.2.1C　深度分析将论证测试文档中所标识的测试足以论证该 TSF 运行是和高层设计和**低层设计**一致的。

评估者行为元素:

ATE _ DPT.2.1E　评估者应当确认所提供的信息满足证据的内容和形式的要求。

ATE _ DPT.3　测试:实现表示

目的:

TSF 的子系统提供这个 TSF 内部工作的一个高层描述。为了论证存在某种缺陷而在这个子系统级别上进行的测试确保已正确实现了该子系统。TSF 的模块提供 TSF 内部工作的描述。为了论证存在某种缺陷而对这个级别的模块进行的测试确保已正确实现了这些 TSF 模块。TSF 的实现表示提供有关该 TSF 内部工作的详细描述。为了论证存在某种缺陷而对这个实现级别进行的测试确保已正确实现了这些 TSF 实现。

应用注释:

我们期望开发者根据"子系统"来描述对该 TSF 高层设计的测试。"子系统"这个术语用来表示把 TSF 分解成数目相对较少的几部分这一概念。

我们期望开发者根据"模块"来描述对该 TSF 低层设计的测试。"模块"这个术语用来表示把 TSF 每个"子系统"分解成数目相对较少的几部分这一概念。

实现表示是用来产生 TSF 本身的(比如待编译的源码)。

依赖关系:

ADV _ HLD.2　安全加强的高层设计

ADV _ IMP.2　TSF 实现

ADV _ LLD.1　描述性低层设计

ATE _ FUN.1　功能测试

开发者行为元素:

ATE _ DPT.3.1D　开发者应提供测试深度的分析。

证据的内容和形式元素：

ATE_DPT.3.1C 深度分析应论证测试文档中所标识的测试足以论证该 TSF 是根据高层设计、低层设计和实现表示而运作的。

评估者行为元素：

ATE_DPT.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的要求。

14.3 功能测试（ATE_FUN）

目的：

开发者进行的功能测试，确保 TSF 表示出的属性必须满足它的 PP/ST 的功能要求。这样的功能测试保证了 TSF 至少能够满足安全功能的要求，尽管它不能确定 TSF 仅仅执行了规定的要求。“功能测试”子类关注的是所要求的文档或支持工具的类型和数量，以及通过开发者的测试所要论证的东西。功能测试并不局限于正面确认已提供必须的安全功能，它还包括校验那些未预期的行为（一般是违反功能要求的）存在与否的反面测试。

本子类有助于保证未发现的缺陷出现的可能性相对较小。

ATE_COV 子类、ATE_DPT 子类 和 ATE_FUN 子类的组合用于定义由开发者提供的测试证据。ATE_IND 专指评估者的独立性功能测试。

组件分级：

本子类包含两个组件，较高层的组件要求分析顺序依赖性。

应用注释：

执行测试的程序最好能提供测试程序和测试工具的使用说明书，包括测试环境、测试条件、测试数据参数和值。测试过程还应该显示如何从测试输入得到测试结果。

该子类为所有测试计划、程序和结果的表示规定了要求。这样，需提出的信息量将根据 ATE_COV 和 ATE_DPT 的使用情况而改变。

当某特定测试的成功执行依赖于某个特定状态的存在时，顺序依赖性就十分重要了。例如：可能要求测试 B 必须紧接在测试 A 之后执行，因为 A 的成功执行是 B 成功执行的必要条件。这样，测试 B 的失败可能与顺序依赖性问题有关。在上面的例子中，测试 B 的失败可能是由于测试 C（而不是测试 A）直接在它之前执行，也可能是与测试 A 的失败有关。

ATE_FUN.1 功能测试

目的：

本组件的目的是由开发者论证所有的安全功能按照规定执行。开发者需要执行测试和提供测试文档。

依赖关系：

无依赖关系。

开发者行为元素：

ATE_FUN.1.1D 开发者应当测试 TSF，并文档化结果。

ATE_FUN.1.2D 开发者应提供测试文档。

证据的内容和形式元素：

ATE_FUN.1.1C 测试文档应当包括测试计划、测试程序描述，预期的测试结果和实际的测试结果。

ATE_FUN.1.2C 测试计划应当标识要测试的安全功能，描述要执行的测试目标。

ATE_FUN.1.3C 测试过程描述应当标识要执行的测试，并描述每个安全功能的测试概况，这些概况

包括对于其他测试结果的顺序依赖性。

ATE _ FUN.1.4C 预期的测试结果应当表明成功测试运行后的预期输出。

ATE _ FUN.1.5C 开发者执行测试的结果应当论证了每个被测试的安全性功能已按照规定进行运作了。

评估者行为元素：

ATE _ FUN.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE _ FUN.2 顺序的功能测试

目的：

本组件的目的是由开发者论证所有的安全功能已按照规定执行了。开发者要求执行测试和提供测试文档。

在本组件中，另一个目的是确保测试是按以下方式构造的：要避免被测 TSF 的某些部分正确性的循环论证。

应用注释：

尽管测试程序可以根据测试顺序陈述初始测试的前提条件，但可能不对排序提供根据。对于测试顺序的分析是决定测试充分性的一个重要因素，因为在测试的排序中有掩盖缺陷的可能性。

依赖关系：

无依赖关系。

开发者行为元素：

ATE _ FUN.1.1D 开发者应当测试 TSF，并文档化结果。

ATE _ FUN.1.2D 开发者应提供测试文档。

证据的内容和形式元素：

ATE _ FUN.1.1C 测试文档应当包括测试计划、测试程序描述，预期的测试结果和实际的测试结果。

ATE _ FUN.1.2C 测试计划应当标识要测试的安全功能，描述要执行的测试目标。

ATE _ FUN.1.3C 测试过程描述应当标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对于其他测试结果的顺序依赖关系。

ATE _ FUN.1.4C 预期的测试结果应当表明成功测试运行后的预期输出。

ATE _ FUN.1.5C 开发者执行测试的结果应当论证了每个被测试的安全性功能已按照规定进行运作了。

ATE _ FUN.2.6C 测试文档应当包含测试程序对顺序依赖性的分析。

评估者行为元素：

ATE _ FUN.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

14.4 独立性测试（ATE _ IND）

目的：

本组件的目的是论证安全功能按照规定执行了。

另外的目的是降低开发者一方对测试结果不正确评定的风险，这些不正确评定将导致规范的不正确实现，或者对不遵照规范的代码的忽略。

组件分级：

本子类的组件分级，是基于测试文档、测试支持和评估者测试的数量。

应用注释：

除评估者之外，该子类中规定的测试还可以由一个有专业知识的团体来支持(如一个独立的实验室、一个客观的用户组织)。测试需要理解 TOE 与其他保证活动的表现的一致性。评估者有责任确保使用这种支持时，也适当指明了该子类的要求。

该子类涉及 TSF 的独立性功能测试所能达到的程度。独立性功能测试可以采用全部或部分重复开发者功能测试的形式，也可采用讨论开发者功能测试的形式，来拓宽开发者测试的深度或广度，或者是测试 TOE 可能有的公开的明显安全性弱点。这些行为是互补的，并且对于每个 TOE 功能都可制定一个适当的组合计划，这个组合考虑了测试结果的可用性和适用范围，以及 TSF 的功能复杂度。一个测试计划要开发到这种程度：即与其他保证行为的级别一致，并且像更高的保证所要求的那样，应包括更多样本的重复测试，更多的由评估者实施的正面和反面功能测试。

对开发者测试的抽样是为了提供这样的确认：即开发者已经开展了他所计划的对于 TSF 的测试程序，并正确记录了结果。抽样的多少受开发者功能测试结果的细节和质量的影响。评估者同样需要考虑设计额外测试的范围，以及以上两方面所带来的有关利益。我们知道，重复所有开发者测试，在某些情况下，也许是可行的，也是我们所希望的，但是在其他情况下比较费力而且低效。所以本子类内的最高级组件应当谨慎使用。抽样可以包含整个可用的测试结果，包括满足 ATE_COV 和 ATE_DPT 的要求的那些结果。

在评估中，TOE 的不同配置也是要考虑的。评估者必须评定所提供结果的可用性，并可相应地制定他自己的测试计划。

独立性功能测试与穿透性测试不同，后者基于在设计或实现中对一个已知的系统的脆弱性进行搜索。穿透性测试将用子类 AVA_VLA 来规定。

TOE 的测试适应性基于对 TOE 的访问，以及用来运行测试的支持文档和所需信息(包括任何测试软件或工具)。这种支持的需要由对其他保证子类的依赖关系来指出。

另外，TOE 的测试适应性也可基于其他考虑，例如开发者提交的版本不一定是最后版本。

对 TSF 子集的引用是旨在允许评估者设计一个适合的测试集合，它与当前实施的评估目的相一致。

ATE_IND.1　独立性测试——一致性

目的：

本组件的目的是论证安全功能按规范运行。

应用注释：

这个组件并不指明开发者测试结果的用途。当这些测试结果不可用时，或开发者的测试未经校验就接受时，这个组件就是适用的。评估者要以确认 TOE 的安全功能要求得到满足为目的来设计和实施测试。这样的方法是为了通过有代表性的测试来取得正确运行的信心，而不是实施每一个可能的测试。为了此目的而计划的测试的程度是一个方法论的问题，需要在特定的 TOE 上下文同其他评估行为的平衡中考虑。

依赖关系：

ADV_FSP.1　非形式化功能规范

AGD_ADM.1　管理员指南

AGD_USR.1　用户指南

开发者行为元素：

ATE_IND.1.1D　开发者应当提供用于测试的 TOE。

证据的内容和形式元素：

ATE_IND.1.1C　TOE 应与测试相适应。

评估者行为元素：

ATE _ IND.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE _ IND.1.2E 评估者应当适当测试一个 TSF 子集，以确认相应的 TOE 按照规范运行。

ATE _ IND.2 独立性测试——抽样

目的：

本组件的目的是论证安全功能按规范运行。评估者测试包括选择和重复测试一个开发者的抽样。

应用注释：

开发者应当为评估者提供能有效重现开发者测试的必需的资料，可能包括像可用计算机处理的测试文档、测试程序等。

这个组件包含这样一个要求：即评估者应拥有开发者提供的可用测试结果以补充测试程序。评估者将重复开发者测试的一个抽样以给出测试结果可信度。要建立上述的信任度，评估者将在开发者测试的基础上执行以另一种方式运行 TOE 的额外的测试。在给定资源的情况下，使用校验开发者测试结果的平台比仅使用开发者自己的测试，能使评估者获得在更大的范围内 TOE 的正确运作的信任度。具有给出开发者已测试 TOE 后的信任度，评估者也将在适当的时候有更多的自由，从而专注于某些领域的测试，比如说文档检查的领域或专业知识已提高到特别的关注程度的领域。

依赖关系：

ADV _ FSP.1 非形式化功能规范

AGD _ ADM.1 管理员指南

AGD _ USR.1 用户指南

ATE _ FUN.1 功能测试

开发者行为元素：

ATE _ IND.2.1D 开发者应当提供用于测试的 TOE。

证据的内容和形式元素：

ATE _ IND.2.1C TOE 应与测试相适应。

ATE _ IND.2.2C 开发者应提供一个与开发者的 TSF 功能测试中使用的资源相当的集合。

评估者行为元素：

ATE _ IND.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE _ IND.2.2E 评估者应当适当测试一个 TSF 子集，以确认 TOE 相应的按照规范运行。

ATE _ IND.2.3E 评估者应抽样执行测试文档里的测试样本，以验证开发者测试的结果。

ATE _ IND.3 独立性测试——全部

目的：

目的是论证所有的安全功能按规范执行，评估者测试包括重复所有的开发者测试。

应用注释：

开发者应当提供给评估者能有效重现开发者测试的必需的资料，可能包括像可用计算机处理的测试文档、测试程序等。

在本组件中评估者必须重复所有的开发者测试，以作为测试程序的一个部分。像前面的组件一样，评估者也将实施测试，但致力于用一种不同于开发者所完成的方式测试 TOE。在开发者测试非常详尽的情况下，以另一种方式测试 TOE，留下的余地非常小。

依赖关系：

ADV _ FSP.1 非形式化功能规范

AGD _ ADM.1 管理员指南

AGD _ USR.1 用户指南

ATE _ FUN.1　功能测试

开发者行为元素：

ATE _ IND.3.1D　开发者应提供用于测试的 TOE。

证据的内容和形式元素：

ATE _ IND.3.1C　TOE 应与测试相适应。

ATE _ IND.3.2C　开发者应提供一个与开发者的 TSF 功能测试中资源相等的一个子集。

评估者行为元素：

ATE _ IND.3.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE _ IND.3.2E　评估者应当适当测试一个 TSF 子集，以确认 TOE 相应的按照规范运行。

ATE _ IND.3.3E　评估者应当执行在测试文档里所有的测试，以验证开发者测试的结果。

15　AVA 类：脆弱性评定

本类讨论可被利用的隐蔽信道的存在性、TOE 的误用或不正确设置的可能性、击败概率或排列机制的可能性以及在 TOE 的开发和运行中引入可利用脆弱性的可能性。

图 15.1 给出本类包含的子类，以及子类中的组件层次：

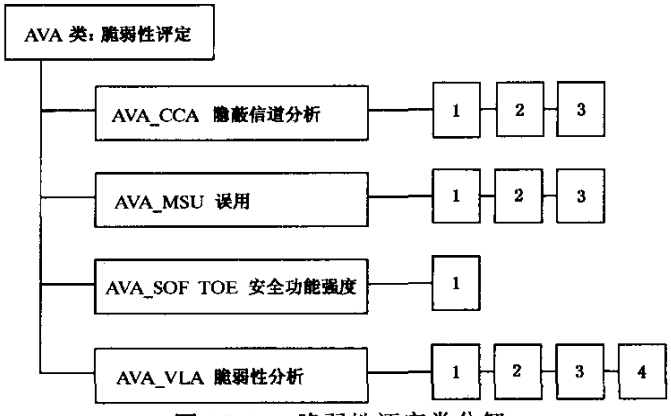

图 15.1　脆弱性评定类分解

15.1　隐蔽信道分析(AVA _ CCA)

目的：

隐蔽信道分析的目的在于确定非预期的信号信道(例如非法信息流)的存在性及其潜在的容量。

保证要求提出了非预期的和可利用的信号信道在违反 SFP 运行时造成的威胁。

组件分级：

组件分级基于隐蔽信道分析不断增加的严格程度。

应用注释：

信道容量的估计基于非形式化的工程量度和实际的测量。

隐蔽信道分析所基于的假设可以包括处理器速度、系统或网络配置、内存大小和缓存大小。

通过测试对隐蔽信道的精细选择分析验证，使得评估者有机会验证隐蔽信道分析的任一方面(例如，识别、容量估计、消除、监视和利用等方案)。这里并没有强加一种要求来论证整套隐蔽信道分析结果。

如果在 ST 中没有信息流控制 SFP，本子类保证要求就不再可用，因为本子类仅仅适用于信息流控

制 SFP。

AVA _ CCA.1　隐蔽信道分析

目的：

通过对隐蔽信道的非形式化搜索，标识出可标识的隐蔽信道。

依赖关系：

ADV _ FSP.2　完全定义的外部接口

ADV _ IMP.2　TSF 实现

AGD _ ADM.1　管理员指南

AGD _ USR.1　用户指南

开发者行为元素：

AVA _ CCA.1.1D　开发者对每个信息流控制策略都应当搜索隐蔽信道。

AVA _ CCA.1.2D　开发者应当提供隐蔽信道分析的文档。

证据的内容和形式元素：

AVA _ CCA.1.1C　分析文档应当标识出隐蔽信道并且估计它们的容量。

AVA _ CCA.1.2C　分析文档应当描述用于确定隐蔽信道存在的程序，以及进行隐蔽信道分析所需要的信息。

AVA _ CCA.1.3C　分析文档应当描述隐蔽信道分析期间所作的全部假设。

AVA _ CCA.1.4C　分析文档应当描述在最坏的情况下对通道容量进行估计的方法。

AVA _ CCA.1.5C　分析文档应当描述每个可标识的隐蔽信道其最坏的利用情形。

评估者行为元素：

AVA _ CCA.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA _ CCA.1.2E　评估者应当确认隐蔽信道分析的结果表明 TOE 符合其功能要求。

AVA _ CCA.1.3E　评估者应当通过测试选择性地验证隐蔽信道分析。

AVA _ CCA.2　系统化隐蔽信道分析

目的：

目的是通过对隐蔽信道的系统化搜索，标识出可标识的隐蔽信道。

应用注释：

按系统化方法进行隐蔽信道分析，要求开发者以结构化、可重复的方式，而不是一种杂乱无章的方式标识出隐蔽信道。

依赖关系：

ADV _ FSP.2　完全定义的外部接口

ADV _ IMP.2　TSF 实现

AGD _ ADM.1　管理员指南

AGD _ USR.1　用户指南

开发者行为元素：

AVA _ CCA.2.1D　开发者对每个信息流控制策略都应当搜索隐蔽信道。

AVA _ CCA.2.2D　开发者应当提供隐蔽信道分析的文档。

证据的内容和形式元素：

AVA _ CCA.2.1C　分析文档应当标识出隐蔽信道并且估计它们的容量。

AVA _ CCA.2.2C　分析文档应当描述用于确定隐蔽信道存在的程序，以及进行隐蔽信道分析所需要的信息。

AVA _ CCA.2.3C 分析文档应当描述隐蔽信道分析期间所作的全部假设。
AVA _ CCA.2.4C 分析文档应当描述在最坏的情况下对通道容量进行估计的方法。
AVA _ CCA.2.5C 分析文档应当为每个可标识的隐蔽信道描述其最坏的利用情形。
AVA _ CCA.2.6C 分析文档应当提供证据证明用于标识隐蔽信道的方法是系统化的。
评估者行为元素：
AVA _ CCA.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
AVA _ CCA.2.2E 评估者应当确认隐蔽信道分析的结果表明 TOE 符合其功能要求。
AVA _ CCA.2.3E 评估者应当通过测试选择性地验证隐蔽信道分析。

AVA _ CCA.3 彻底的隐蔽信道分析
目的：
目的是通过对隐蔽信道的穷举搜索，标识出可标识的隐蔽信道。
应用注释：
按穷举法进行隐蔽信道分析要求提供额外的证据，表明标识隐蔽信道之后的计划足以确保所有可能的隐蔽信道搜索方法都已执行。
依赖关系：
ADV _ FSP.2 完全定义的外部接口
ADV _ IMP.2 TSF 实现
AGD _ ADM.1 管理员指南
AGD _ USR.1 用户指南
开发者行为元素：
AVA _ CCA.3.1D 开发者对每个信息流控制策略都应当搜索隐蔽信道。
AVA _ CCA.3.2D 开发者应当提供隐蔽信道分析的文档。
证据的内容和形式元素：
AVA _ CCA.3.1C 分析文档应当标识出隐蔽信道并且估计它们的容量。
AVA _ CCA.3.2C 分析文档应当描述用于确定隐蔽信道存在的程序，以及进行隐蔽信道分析所需要的信息。
AVA _ CCA.3.3C 分析文档应当描述隐蔽信道分析期间所作的全部假设。
AVA _ CCA.3.4C 分析文档应当描述在最坏的情况下对通道容量进行估计的方法。
AVA _ CCA.3.5C 分析文档应当为每个可标识的隐蔽信道描述其最坏的利用情形。
AVA _ CCA.3.6C 分析文档应当提供证据证明用于标志隐蔽信道的方法是**穷举法**。
评估者行为元素：
AVA _ CCA.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
AVA _ CCA.3.2E 评估者应当确认隐蔽信道分析的结果表明 TOE 符合其功能要求。
AVA _ CCA.3.3E 评估者应当通过测试精细地选择地验证隐蔽信道分析。

15.2 误用（AVA _ MSU）
目的：
“误用”调查的是 TOE 是否以不安全的方式使用或配置，而管理员或用户却想当然地认为它是安全的。
其目的包括：
a）尽可能减少管理员或用户无法检测到不安全配置和安装 TOE 的可能性；
b）尽可能减少在运行中人为或其他错误的风险，这些错误可能造成安全功能解除、无效、或者无法

激活，导致进入无法检测的不安全状态。

组件分级：

组件分级基于开发者所提供不断增加的证据和不断增加的分析严格性。

应用注释：

冲突、误导、不完备或者不合理的指南可能导致 TOE 的用户在它不安全时认为安全，从而导致脆弱性。

冲突性指南的一个例子是，在提供相同输入的条件下，两条指南的指令会导致不同的输出。

误导性指南的一个例子是，对某一条指南指令的描述可以有不止一种的语法分析，其中一个解释方式会导致不安全状态。

不完备指南的一个例子是，一个重要的物理安全要求的列表中遗漏了重要的一项，导致管理员忽略了该项而认为该列表是完备的。

不合理指南的一个例子是，建议遵循一个程序，而该程序会强加不适当的繁重的管理负担。

指导性文档可被包含在现成的用户或管理员文档内，也可以单独提供。如果单独提供，评估者应确认文档是与 TOE 一起提供的。

AVA _ MSU.1　指南审查

目的：

目的是确保指导性文档中不出现误导性的、不合理的和冲突性的指南，而且对所有运行方式提供了安全程序，更易于检测到不安全状态。

依赖关系：

ADO _ IGS.1　安装、生成和启动过程

ADV _ FSP.1　非形式化功能规范

AGD _ ADM.1　管理员指南

AGD _ USR.1　用户指南

开发者行为元素：

AVA _ MSU.1.1D　开发者应当提供指导性文档。

证据的内容和形式元素：

AVA _ MSU.1.1C　指导性文档应当确定对 TOE 的所有可能的运行方式（包括失败和操作失误后的运行），它们的后果以及对于保持安全运行的意义。

AVA _ MSU.1.2C　指导性文档应当是完备的、清晰的、一致的、合理的。

AVA _ MSU.1.3C　指导性文档应当列出所有目标环境的假设。

AVA _ MSU.1.4C　指导性文档应当列出所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求。

评估者行为元素：

AVA _ MSU.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA _ MSU.1.2E　评估者应当重复所有配置与安装程序，以确认只使用所提供的指导性文档就可以让 TOE 安全配置和使用。

AVA _ MSU.1.3E　评估者应当决定指导性文档的使用能检测到所有不安全状态。

AVA MSU.2　分析确认

目的：

目的是确保指导性文档中不出现误导性的、不合理的、以及冲突性的指南，而且对所有运行方式提供了安全程序，更易于检测到不安全状态。在本组件内，要求开发者分析指导性文档，从而提供达到目的的附加保证。

依赖关系：

ADO _ IGS.1 安装、生成和启动过程

ADV _ FSP.1 非形式化功能规范

AGD _ ADM.1 管理员指南

AGD _ USR.1 用户指南

开发者行为元素：

AVA _ MSU.2.1D 开发者应当提供指导性文档。

AVA _ MSU.2.2D 开发者应当文档化对指导性文档的分析。

证据的内容和形式元素：

AVA _ MSU.2.1C 指导性文档应当确定对 TOE 的所有可能的运行方式(包括失败和操作失误后的运行)，它们的后果以及对于保持安全运行的意义。

AVA _ MSU.2.2C 指导性文档应当是完备的、清晰的、一致的、合理的。

AVA _ MSU.2.3C 指导性文档应当列出所有目标环境的假设。

AVA _ MSU.2.4C 指导性文档应当列出所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。

AVA _ MSU.2.5C 分析文档应当论证指导性文档是完备的。

评估者行为元素：

AVA _ MSU.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA _ MSU.2.2E 评估者应当重复所有配置与安装程序以及其他选择性程序，以确认只使用所提供的指导性文档就可以让 TOE 安全配置和使用。

AVA _ MSU.2.3E 评估者应当决定指导性文档的使用能检测到所有不安全状态。

AVA _ MSU.2.4E 评估者应当决定分析文档说明了为 TOE 所有的运行方式提供了安全运行指南。

AVA _ MSU.3 对非安全状态的分析和测试

目的：

确保指导性文档中不出现误导性的、不合理的、以及冲突的指南，而且对所有运行方式提供了安全规程，更易于检测到不安全状态。在本组件内，要求开发者分析指导性文档，从而提供达到目的的附加保证。而且该分析通过测试的方式得到评估者的验证和确认。

应用注释：

本组件要求评估者进行测试以确保当 TOE 进入不安全状态时，它可容易地被检测到。这一测试可被认为是穿透性测试的一个特别方面。

依赖关系：

ADO _ IGS.1 安装、生成和启动过程

ADV _ FSP.1 非形式化功能规范

AGD _ ADM.1 管理员指南

AGD _ USR.1 用户指南

开发者行为元素：

AVA _ MSU.3.1D 开发者应当提供指导性文档。

AVA _ MSU.3.2D 开发者应当文档化对指导性文档的分析。

证据的内容和形式元素：

AVA _ MSU.3.1C 指导性文档应当确定对 TOE 的所有可能的运行方式(包括失败和操作失误后的运行)，它们的后果以及对于保持安全运行的意义。

AVA _ MSU.3.2C 指导性文档应当是完备的、清晰的、一致的、合理的。

AVA _ MSU.3.3C 指导性文档应当列出所有目标环境的假设。

AVA _ MSU.3.4C 指导性文档应当列出所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。

AVA _ MSU.3.5C 分析文档应当论证指导性文档是完备的。

评估者行为元素：

AVA _ MSU.3.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA _ MSU.3.2E 评估者应当重复所有配置与安装程序以及其他选择性程序，以确认只使用所提供的指导性文档就可以让 TOE 安全配置和使用。

AVA _ MSU.3.3E 评估者应当决定指导性文档的使用能检测到所有不安全状态。

AVA _ MSU.3.4E 评估者应当决定分析文档说明了为 TOE 所有的运行模式提供了安全运行指南。

AVA _ MSU.3.5E 评估者应当进行独立性测试，以确定管理员或用户在理解指导性文档的情况下，能基本判断 TOE 是否在不安全状态下配置或运行。

15.3 TOE 安全功能强度(AVA SOF)

目的：

由于 TOE 底层安全机制中存在脆弱性，即使 TOE 安全功能没有被旁路、失效、或破坏，它还是可能遭到攻击。对于这些安全功能，其安全行为的合格性可以通过对这些机制的安全行为大量的统计分析结果以及为克服脆弱性所付出的努力来形成。该合格性证明是以 TOE 安全功能强度声明的形式来作出的。

组件分级：

在这个子类仅有一个组件。

应用注释：

安全功能通过安全机制实现。例如，口令机制可以用于标识和鉴别安全功能。

TOE 安全功能强度的评估基于安全机制级别，其结果提供了相关的安全功能对抗已标识威胁的能力信息。

TOE 安全功能强度分析至少应当考虑包括 ST 在内的所有 TOE 可交付材料是否满足目标评估的保证级。

AVA _ SOF.1 TOE 安全功能强度评估

依赖关系：

ADV _ FSP.1 非形式化功能规范

ADV _ HLD.1 描述性高层设计

开发者行为元素：

AVA _ SOF.1.1D 开发者应对 ST 中标识的每个具有 TOE 安全功能强度声明的安全机制进行 TOE 安全功能强度分析。

证据的内容和形式元素：

AVA _ SOF.1.1C 对于具有 TOE 安全功能强度声明的每个安全机制，TOE 安全功能强度分析应说明

该机制达到或超过 PP/ST 定义的最低强度。

AVA _ SOF.1.2C 对于具有特定 TOE 安全功能强度声明的每个安全机制，TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 定义的特定功能强度。

评估者行为元素：

AVA _ SOF.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA _ SOF.1.2E 评估者应确认强度声明是正确的。

15.4 脆弱性分析(AVA _ VLA)

目的：

脆弱性分析是一种评定，用来决定在对 TOE 的构建和预期运行进行评估或通过其他方法(例如，缺陷假设)中所标识的脆弱性是否允许用户违反 TSP。

脆弱性分析涉及的是用户能发现缺陷的威胁，这些缺陷会对资源(例如数据)进行非授权访问、影响或修改 TSF、或者干涉其他授权用户的权限。

组件分级：

组件分级基于开发者或评估者进行脆弱性分析时不断增加的严格性。

应用注释：

开发者进行脆弱性分析是为了探知安全脆弱性的存在，因而它至少需要考虑全部 TOE 可交付材料，其中包括与目标评估保证级相应的 ST。要求开发者文档化已标识脆弱性的分布，如果这些信息对于支持评估者的独立脆弱性分析有用，评估者就能够使用这些信息。

开发者分析的意图是确认在 TOE 的目标环境下已标识的脆弱性可以被利用，而且 TOE 可抵抗明显的穿透性攻击。

明显的脆弱性可认为是那些只要求对 TOE 的极少理解、极少技能、极小技术复杂度和极少资源就可以公开利用的脆弱性。这些脆弱性由 TSF 接口描述所提出。明显脆弱性包括开发者可以通过公开渠道获得细节或者从评估机构获得该细节。

系统地进行脆弱性搜索要求开发者按照结构化可重复的方式标识脆弱性，而不是用杂乱无章的方式来标识。系统化搜索的相关证据应当包括搜索脆弱性所基于的全部 TOE 文档的标识。

独立脆弱性分析超出了开发者标识的脆弱性。评估者分析的主要意图是确定 TOE 抵抗具有低等攻击潜力(AVA _ VLA.2)、中等攻击潜力(AVA _ VLA.3)或者高等攻击潜力(AVA _ VLA.4)的攻击者发起的穿透性攻击。为达到这一目的，评估者首先对所有发现的脆弱性的利用进行评估。这是通过执行穿透性测试而完成的。评估者应假设充当具有低等、中等、高等攻击潜力来企图攻击 TOE 的角色。这些攻击者所利用的脆弱性应当被评估者认为是从 AVA _ VLA.2 到 AVA _ VLA.4 的组件中的“明显穿透性攻击”(根据 AVA _ VLA. *.2C 元素)。

AVA _ VLA.1 开发者脆弱性分析

目的：

开发者进行脆弱性分析来确定明显的安全脆弱性的存在，并确认在所期望的 TOE 环境下脆弱性不能被利用。

应用注释：

作为对其他评估部分中标识的潜在可利用的脆弱性的结果，评估者应当考虑执行附加的检验测试。

依赖关系：

ADV _ FSP.1 非形式化功能规范

ADV _ HLD.1　描述性高层设计

AGD _ ADM.1　管理员指南

AGD _ USR.1　用户指南

开发者行为元素：

AVA _ VLA.1.1D　开发者应当分析 TOE 可交付材料，以寻找用户违反 TSP 的明显途径，并将分析结果文档化。

AVA _ VLA.1.2D　开发者应当文档化明显的脆弱性分布。

证据的内容和形式元素：

AVA _ VLA.1.1C　对所有已标识的脆弱性，文档应当能说明在所期望的 TOE 环境中无法利用这些脆弱性。

评估者行为元素：

AVA _ VLA.1.1E　评估者应当确认提供的信息满足证据的内容和形式的所有要求。

AVA _ VLA.1.2E　评估者应当在开发方脆弱性分析的基础上实施穿透性测试，确保已经表述了明显的脆弱性。

AVA _ VLA.2　独立脆弱性分析

目的：

开发者通过脆弱性分析来确定安全脆弱性的存在，并确认在所期望的 TOE 环境下无法利用这些脆弱性。

在独立脆弱性的分析支持下，评估者进行独立穿透性测试来确定 TOE 可以抵御具有低等攻击潜力的攻击者发起的穿透性攻击。

依赖关系：

ADV _ FSP.1　非形式化功能规范

ADV _ HLD.2　安全加强的高层设计

ADV _ IMP.1　TSF 实现的子集

ADV _ LLD.1　描述性低层设计

AGD _ ADM.1　管理员指南

AGD _ USR.1　用户指南

开发者行为元素：

AVA _ VLA.2.1D　开发者应当分析 TOE 可交付材料，以寻找用户违反 TSP 的途径，并将分析结果文档化。

AVA _ VLA.2.2D　开发者应当文档化已标识的脆弱性的分布。

证据的内容和形式元素：

AVA _ VLA.2.1C　对所有已标识的脆弱性，文档应当能说明在所期望的 TOE 环境中无法利用这些脆弱性。

AVA _ VLA.2.2C　文档应当证明对于具有已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。

评估者行为元素：

AVA _ VLA.2.1E　评估者应当确认提供的信息满足证据的内容和形式的所有要求。

AVA _ VLA.2.2E　评估者应当在开发方脆弱性分析的基础上实施穿透性测试，确保已经表述了标识明显的脆弱性。

AVA _ VLA.2.3E　评估者应当实施独立的脆弱性分析。

AVA _ VLA.2.4E　基于独立的脆弱性分析，评估者应当实施独立的穿透性测试以决定在所期望环境下额外标识的脆弱性的可利用性。

AVA _ VLA.2.5E 评估者应当决定可以抵御具有低等攻击潜力的攻击者发起的对 TOE 的穿透性攻击。

AVA _ VLA.3 中级抵抗力

目的：

开发者通过脆弱性分析来确定安全脆弱性的存在，并确认在所期望的 TOE 环境下无法利用这些脆弱性。

在独立脆弱性分析的支持下，评估者进行独立穿透性测试来确定 TOE 可以抵御具有中等攻击潜力的攻击者发起的穿透性攻击。

依赖关系：

ADV _ FSP.1 非形式化功能规范
ADV _ HLD.2 安全加强的高层设计
ADV _ IMP.1 TSF 实现的子集
ADV _ LLD.1 描述性低层设计
AGD _ ADM.1 管理员指南
AGD _ USR.1 用户指南

开发者行为元素：

AVA _ VLA.3.1D 开发者应当分析 TOE 可交付材料，以寻找用户违反 TSP 的途径，并将分析结果文档化。
AVA _ VLA.3.2D 开发者应当文档化已标识的脆弱性的分布。

证据的内容和形式元素：

AVA _ VLA.3.1C 对所有已标识的脆弱性，文档应当能说明在所期望的 TOE 环境中无法利用这些脆弱性。
AVA _ VLA.3.2C 文档应当证明对于具有已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。
AVA _ VLA.3.3C 证据应当能说明对脆弱性的搜索是系统化的。

评估者行为元素：

AVA _ VLA.3.1E 评估者应当确认提供的信息满足证据的内容和形式的所有要求。
AVA _ VLA.3.2E 评估者应当在开发方脆弱性分析的基础上实施穿透性测试，确保已经表述了标识明显的脆弱性。
AVA _ VLA.3.3E 评估者应当实施独立的脆弱性分析。
AVA _ VLA.3.4E 基于独立的脆弱性分析，评估者将应当实施独立的穿透性测试以决定在所期望环境下额外标识的脆弱性的可利用性。
AVA _ VLA.3.5E 评估者应当决定可以抵御具有中等攻击潜力的攻击者发起的对 TOE 的穿透性攻击。

AVA _ VAL.4 高级抵抗力

目的：

开发者通过脆弱性分析来确定安全脆弱性的存在，并确认在所期望的 TOE 环境下无法利用这些脆弱性。

在独立脆弱性的分析支持下，评估者进行独立穿透性测试来确定 TOE 可以抵御具有高等攻击潜力的攻击者发起的穿透性攻击。

依赖关系：

ADV _ FSP.1 非形式化功能规范

ADV _ HLD.2　安全加强的高层设计
ADV _ IMP.1　TSF 实现的子集
ADV _ LLD.1　描述性低层设计
AGD _ ADM.1　管理员指南
AGD _ USR.1　用户指南

开发者行为元素：

AVA _ VLA.4.1D　开发者应当分析 TOE 可交付材料，以寻找用户违反 TSP 的途径，并将分析结果文档化。
AVA _ VLA.4.2D　开发者应当文档化已标识的脆弱性的分布。

证据的内容和形式元素：

AVA _ VLA.4.1C　对所有已标识的脆弱性，文档应当能说明在所期望的 TOE 环境中无法利用这些脆弱性。
AVA _ VLA.4.2C　文档应当证明对于具有已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。
AVA _ VLA.4.3C　证据应当能说明对脆弱性的搜索是系统化的。
AVA _ VLA.4.4C　分析文档应当提供完备地分析表述 TOE 可交付材料的证明。

评估者行为元素：

AVA _ VLA.4.1E　评估者应当确认提供的信息满足证据的内容和形式的所有要求。
AVA _ VLA.4.2E　评估者应当在开发方脆弱性分析的基础上实施穿透性测试，确保已经表述了标识明显的脆弱性。
AVA _ VLA.4.3E　评估者应当实施独立的脆弱性分析。
AVA _ VLA.4.4E　基于独立的脆弱性分析，评估者将应当实施独立的穿透性测试以决定在所期望环境下额外标识的脆弱性的可利用性。
AVA _ VLA.4.5E　评估者应当决定可以抵御具有高等攻击潜力的攻击者发起的对 TOE 的穿透性攻击。

16　保证维护范例

16.1　引言

本章针对保证维护类(AMA)所支持的保证维护范例进行论述。它为理解应用 AMA 要求的一个可能途径提供了有用的信息。

保证维护是一个概念，应用在一个 TOE 已经根据第 5～6 章和第 9～15 章的标准被评估和认证之后。保证维护的要求旨在保证当 TOE 或其环境发生变化时，能够继续满足安全目标。这样的变化包括发现新的威胁或者易受攻击的脆弱性、在用户要求方面的变化、纠正已认证 TOE 中所发现的错误、以及其他提供的功能的变化。

决定保证已进行维护的一个方法是再次评估 TOE。术语“再次评估”在这里指的是对新版本的 TOE 进行评估，它包括对已认证版本 TOE 的安全相关性变化，以及对那些仍然有效的评估结果的再次利用。然而在许多情况下，对每个 TOE 的新版本进行再次评估而得到保证维护，这是不现实的。

因此，AMA 类的主要目的是定义一整套要求，这套要求提供一个信任度，在 TOE 中建立的保证得到了维护，而并不总需要进行形式化的 TOE 新版本的再次评估。AMA 类并没有完全去除对再次评估的要求。在某些情况下，变化的影响是如此重要以至于只有通过再次评估才能确保已经维护了保证。这个类的要求还有另一个目的，必要时支持对 TOE 值当的再次评估。

值得注意的是，在不满足任何 AMA 要求的情况下，可以根据第 5～6 章和第 9～15 章的标准对 TOE 新版本进行再次评估。然而，AMA 类包括支持这些再次评估中使用的要求。

保证维护的开发者和评估者行为，只有在 TOE 进行评估和证明之后才能加以应用，虽然如下面所描述的那样，一些要求能在评估的时候就加以应用。为清楚起见，在这个范例的表述中使用了下面的术语：

a) TOE*已认证版本* 指的已经进行评估和认证的版本；

b) TOE*当前版本* 指的是与已认证版本在某些方面不同的的版本；这可以是：

——TOE 的新的版本；

——纠正了已发现错误的已认证版本；

——同样的基本 TOE 版本，但是在不同的硬件或者软件平台上。

开发者与评估者在这个类中的角色如 GB/T 18336.1 中所描述。然而，在本类中所指的评估者并不一定就是已评估的 TOE 认证版本中的评估者。

为了让保证在 TOE 中得到维护，而不总是需要进行形式化的再次评估，本类的要求对开发者提出了这样的义务：即保留证据来说明 TOE 仍然满足它的安全目标（例如开发者测试证据）。

16.2 保证维护周期

本条描述使用保证维护子类及其组件的一个可能的方法，并且举例说明这个概念的用法。这个例子是一个“保证维护周期”模型，而且可以划分成下列的三个阶段：

a) *接受阶段*，周期的开始阶段，开发者在周期内建立保证维护的计划和程序，并得到评估者的独立验证；

b) *监视阶段*，在这一阶段，开发者在周期内提供一点或多点证据来证明根据已建立的计划和程序，TOE 的保证得到了维护，这种保证维护证据由评估者独立进行检验；

c) *再次评估阶段*，结束周期，在这一阶段，基于从已认证版本以来影响 TOE 的变化提交一个更新的版本，以便于再次评估。

AMA 内的子类主要阐述上面前两个阶段，同时为第三阶段提供支持。这里引入这些阶段仅仅是为了帮助描述保证维护要求的应用，并没有要求保证维护方案正式包含这些阶段。

保证维护周期如图 16.1 所示。

在这个例子中，只有在顺利完成接受阶段之后 TOE 才能进入监视阶段（即开发者进行保证维护的计划和程序被接受）。如果开发者在监视阶段内对这些计划或者程序进行了更改，TOE 将需要重新进入接受阶段以便接受这些更改。

在监视阶段内，开发者遵循保证维护的计划与程序，执行影响 TOE 变化的安全因素分析（安全影响分析）。在这个阶段内的某些时候，评估者独立地检查（借助于审计）开发者的工作。开发者应保证遵循计划和程序，并且正确完成安全影响分析。

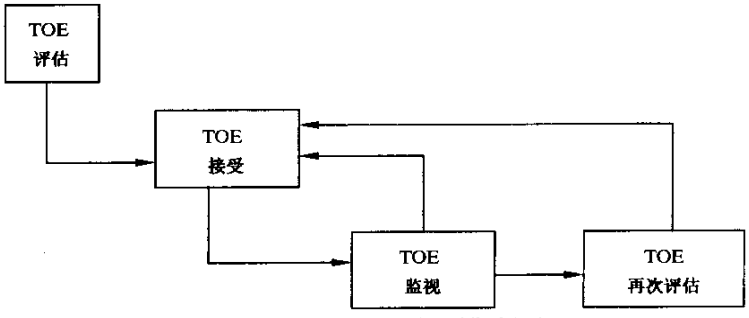

图 16.1 保证维护周期例子

因此，一旦 TOE 处于监视阶段，就有可能对开发者提供的 TOE 新版本进行保证维护有个信任度。受改变的 TOE 经过某一不确定的时间段就不能继续处于监视阶段：在某些时刻，对 TOE 的再次

评估是必要的。何时需要再次评估，取决于 TOE 的累积变化和特别重大的变化。比如，大量的小变化对保证的影响等同于一个大变化。开发者的保证维护的计划中定义了在监视阶段可能影响 TOE 的变化范围(参见下面的 16.3.1 部分)。

类似地，在监视阶段也不可能改进 TOE(比如提高保证级)；这只有通过对 TOE 的评估才能获得(对以前的评估加以适当的再利用)。

如果发现未能遵循保证维护程序，并且因此削弱了 TOE 的保证，TOE 的保证维护状态必须重新复查。在某些情况下，开发者可能被要求为提交 TOE 进行再次评估，然后开始新的保证维护周期。

16.2.1 TOE 的接受

在本例中，保证维护周期的 TOE 接受阶段可细分如下(见图 16.2)，这一细分使用了 AMA 类的保证维护计划和 TOE 组件分类报告子类：

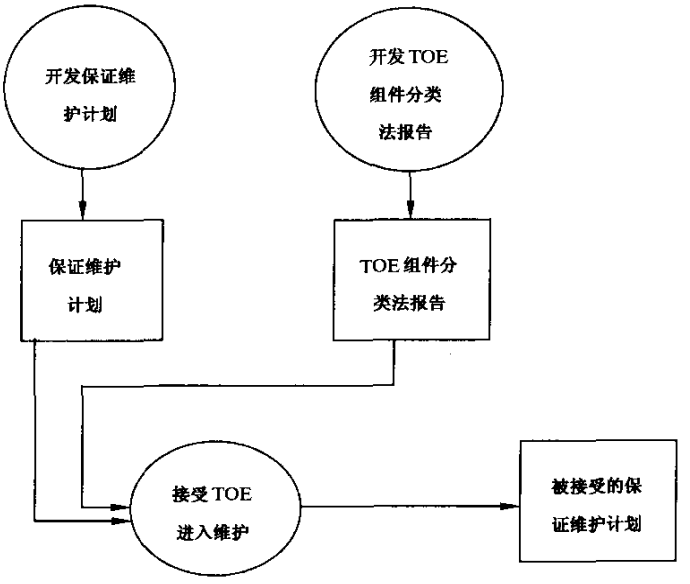

图 16.2 TOE 接受方式例子

16.2.2 TOE 的监视

保证维护周期的 TOE 监视阶段可细分如下(见图 16.3)，这一细分使用了 AMA 类的保证维护证据和安全影响分析子类：

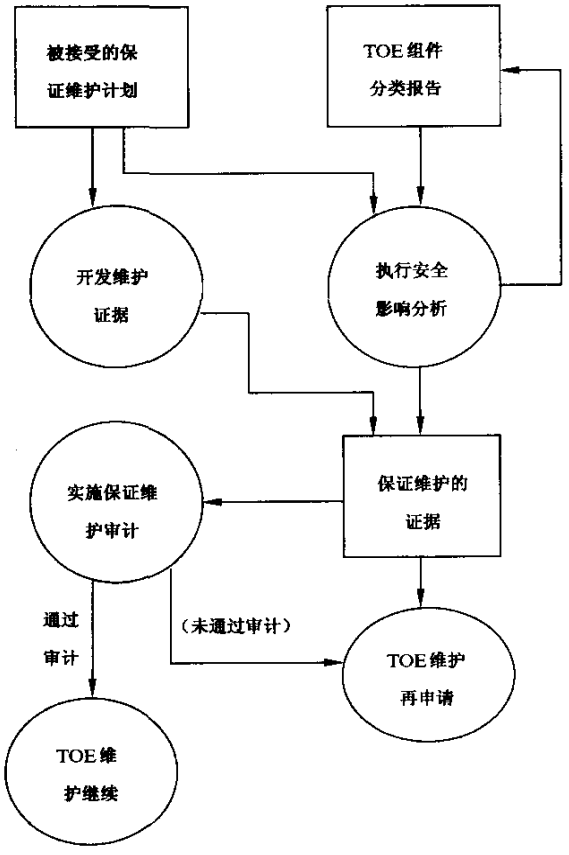

图 16.3　TOE 监视方式例子

16.2.3　再次评估

这个维护周期例子的第三阶段是再次评估阶段，评估者利用影响分析和保证维护的证据，以及适用于对象保证级的保证组件，来重新检查 TOE 的各个部分。

再次评估活动可列入 AM 计划，它要求响应不可预见的 TOE 或其环境的重大变化而使保证维护活动被认为是不适当的。

16.3　保证维护的类和子类

为了支持不同的保证维护方法而开发的 AMA 类，如表 16.1 所示的四子类组成：

表 16.1　保证维护的细分和对应关系

保证类	保证子类	缩写名
AMA 类：保证维护	保证维护计划	AMA _ AMP
	TOE 组件分类报告	AMA _ CAT
	保证维护证据	AMA _ EVD
	安全影响分析	AMA _ SIA

16.3.1　保证维护计划

AM 计划对评估结果和 TOE 组件分类定义，提供了清晰的保证维护的基线。

当 TOE 和其环境发生改变时，为确保在认证 TOE 中建立的保证能够得到维护，保证维护计划(AM 计划)标识出开发者实现的计划和程序。AM 计划覆盖整个保证维护周期。

AM 计划定义了 TOE 变化的范围，而不会引起再次评估。要遵循的特定方式是与方案相关的，但是下列类型的变化很有可能是在 AM 计划范围外，只能用再次评估来表述：

a) 安全目标的重要变化（如安全环境、安全目标或者安全功能要求的重大变化，或者增加*任何*保证要求）；

b) 类型为*实施* TSP 的外部 TSF 接口的重要变化；

c) （保证要求包括 ADV_HLD.1 或者更高级组件时）类型为 TSP 实施的 TSF 子系统的重要变化。

需要注意的是，在维护条件下，变更的方式可能受 TOE 提供的功能的影响，使得已评估的配置安全自动生效。这些功能可以防止对一个可运行的 TOE 的不适当的或破坏性的变化。

由于对构成一个*重大*变化的定义不仅仅取决于被评估 TOE 的类型和安全目标的内容，所以 GB/T 18336不包括对以上规则更精确的规定。

在保证维护周期内，为了确保 TOE 的保证得到维护，需要 AM 计划定义或者引用即将被应用的程序。有四类程序被认为是必须应用的：

a)配置管理程序，它控制并记录 TOE 的变化以支持开发者的安全影响分析，当然它还支持文档（包括 AM 计划本身）；

b) 维护“保证证据”的程序（比如适当的保证要求所需的文档证据的维护），这是对 TOE 安全功能测试的关键方面，对开发者的回归测试策略来说更是这样；

c) 控制对影响 TOE 的变化进行安全影响分析的程序（注意，这些变化包括 TOE 环境内的变化，例如需标识并追踪的新的威胁和攻击方法），以及控制变化发生时对 TOE 组件分类报告的维护的程序；

d) 缺陷纠正程序，它包括追踪并更正已经报告了的安全缺陷（如 ALC_FLR.1 所要求）。

AM 计划希望在保证维护周期结束（即计划的再次评估的结束）前一直保持有效，之后将会要求新的 AM 计划。当开发者不遵循计划，或者作出不在计划范围内的变更，或者为了让 TOE 在其环境中继续有效而不得不作出这些变更时，AM 计划将被认为不再有效。在 TOE 进入新的监视阶段之前需要重新提交和接受更新了的 AM 计划。

AM 计划要求开发者指定开发方安全分析员来监视安全维护过程。这一角色可以由多个人员组成。开发方安全分析员应该熟悉 TOE、评估结果以及可用的保证要求，这是胜任该角色的主要先决条件。至于该级别上的知识和经验是如何获得的，计划要求并未指定。然而有可能的是，将来的开发方安全分析员必须经过某些形式的培训以弥补他或她知识和经验的不足。开发方安全分析员在开发方的组织内应该具有足够的威信，这样才可以确保 AM 计划和与之相关教程的要求得到遵循。

16.3.2 TOE 组件分类报告

TOE 组件分类报告的目的，是通过提供对 TOE 组件（例如 TSF 子系统）的分类来补充 AM 计划，其组件是基于它们的安全相关性的。这个分类在开发方安全影响分析以及随后的 TOE 再次评估中处于中心地位。

对 TOE 组件的分类报告的检查发生在接受阶段；评估者仅检查关于已认证版本的 TOE 的报告的版本。尽管 AM 计划中的保证维护程序，要求开发者在对 TOE 进行更改后更新 TOE 组件分类报告，评估者并不必重新分析文档；然而，这些更新很可能在监视阶段受到检查。

TOE 组件分类报告包括了被维护的保证级上的所有 TSF 表示。TOE 组件分类报告还指出：

a) TOE 外部的而且满足定义于 ST 中的 IT 安全要求的任何硬件、固件和软件组件（例如硬件或软件平台）；

b) 一旦被更改，将对 TOE 满足其 ST 所需的保证有影响的任何开发工具。

TOE 组件分类报告还描述了 TOE 组件分类所采用的方法。至少，TOE 组件应被归类到 TSP 实施和非 TSP 实施两个类中。对分类方法的说明旨在允许开发方安全分析员决定把新 TOE 组件分给哪一类，或者在 TOE 或者其 ST 的变化发生后如何改变已有 TOE 组件的分类。

对 TOE 组件的初始分类将基于协助进行 TOE 评估的开发者所提供的证据，并由评估者独立证实。尽管对文档的维护是开发方安全分析员的职责，但它最初的内容是基于 TOE 评估的结果。

当未来版本的 TOE 要求维护保证时，把 AMA _CAT.1 包括在 ST 内是有好处的。其应用时，并不理会保证维护是通过应用本类的要求得到的，还是对 TOE 进行周期性再次评估得到。

16.3.3 保证维护证据

要建立必须的信任度确信 TOE 中的保证正在由开发者根据 AM 计划进行维护。这可以通过提供证据来实现，这些证据说明 TOE 中的保证已进行维护，并由评估者对它独立检查。这一检查（术语为“AM 审计”）在 TOE 保证维护周期的监视阶段通常被周期性采用。

AM 审计的执行，是根据定义于 AM 计划中的调度表。因此，在保证维护周期的监视阶段，由 AMA _EVD.1 所要求的开发者和评估者活动将被调用一次或多次。评估者可能要访问 TOE 开发环境以检查所要求的证据，但同时并不排斥用其他方式进行检查。

开发者要求提供证据表明 AM 计划中提到的保证维护规程得到了执行。这包括：

a）配置管理记录；

b）安全影响分析所涉及的文档，包括当前版本 TOE 组件分类报告、所有可用的保证要求的证据例如设计更新、测试文档、新版本指南文档等等；

c）安全缺陷追踪的证据。

评估者对于开发者的安全影响分析（由 AMA _EVD.1 所依赖的 AMA _SIA.1 要求）的检查作为 AM 审计的主要部分。接着，AM 审计提供开发者分析的确证（和分析质量的可信度），这样有助于验证开发者的声明，即在当前版本 TOE 中保证得到了维护。

AM 审计要求评估者确认在 TOE 的当前版本上完成了功能性测试。因为测试文档提供可靠的证据说明 TOE 安全功能按指定方式继续运行，这一要求作为单独的检查以示强调。评估者抽样测试文档以确认开发者测试表明安全功能按指定方式运转，而且测试的广度和深度与维护的保证级是相一致的。

16.3.4 安全影响分析

安全影响分析的目的是提供保证在 TOE 中得到维护的可信度，这一目的是通过开发者针对自从认证以来影响 TOE 所有变化的安全影响分析而达到的。这些要求可以在监视阶段或者再次评估阶段得到应用。

开发者的安全影响分析基于 TOE 的组件分类报告：对于 TSP 实施的 TOE 组件的变更将导致难以保证变更后的 TOE 满足 ST。因此，所有的这些变更，要求对它们的安全影响进行分析，以说明它们没有减弱 TOE 的保证。

本子类的组件可用于支持其后的 AM 审计或 TOE 的再次评估。

对于 AM 审计，评估者对安全影响分析的评审将作为以后审计活动的重点，也进一步确认了开发者的分析。

安全影响分析根据哪些 TOE 组件是新的，哪些组件被修改来标识认证版本 TOE 的变化。评估者在相关的 AM 审计或在相关的 TOE 再次评估时验证这些信息的准确性。

提供支持再次评估的安全影响分析，可以减少 TOE 建立要求的保证级时评估者所花费的努力。对 AMA _SIA.2（它要求对安全影响分析进行完整检查）的应用将会为再次评估提供最大的利益。评估机构希望在再次评估实践中使用的安全影响分析的环境的精确详细的描述超出了 GB/T 18336 的范围。

17 AMA 类：保证维护

保证维护类提出的要求必须在 TOE 针对 GB/T 18336 认证之后才可以应用。这些要求旨在确保 TOE 或其环境变更后，继续满足安全目标。这些变更包括新的威胁和脆弱性的发现、用户要求的变更、以及认证过的 TOE 中错误的更正。

本类包含四个子类，子类内的组件层次如图 17.1 所示：

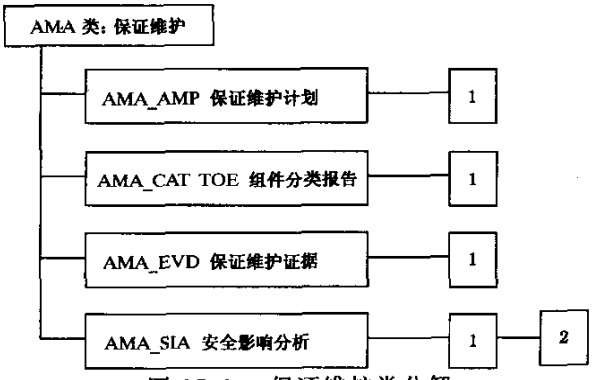

图 17.1　保证维护类分解

17.1　保证维护计划(AMA _ AMP)

目的：

保证维护计划(AM 计划)标识了开发者必须实现的计划和程序，以确保当 TOE 或其环境发生变动时已认证的 TOE 的保证得到了维护。AM 计划对 TOE 来说是特有的，并被剪切到开发方自己的实践和程序内。

组件分级：

这个子类仅包含一个组件。

应用注释：

一个 AM 计划包括一个保证维护周期，也就是从对 TOE 的最近一次评估完成到计划中下一次再次评估的完成。

AMA _ AMP. 1. 2C 和 AMA _ AMP. 1. 3C 要求根据评估结果和对 TOE 组件分类的定义来提供一个清晰的保证维护的基线。TOE 组件分类报告是 AMA _ CAT 子类要求的主体，并作为开发方安全分析员执行安全影响分析的基础。

AMA _ AMP. 1. 4C 要求根据可能改变的 TOE 组件分类和可能改变的表示级别来定义计划所覆盖的变动范围(参考 TOE 组件分类报告的相关部分)。

AMA _ AMP. 1. 5C 要求开发方提供对于任何新版本 TOE 的*当前*计划的描述。这些计划改变可能会改变，因而要求一个更新的 AM 计划。然而，应当注意，在本文上下文中术语*新版本*不包含有修正了的错误的次要(未计划的)TOE 版本。

AMA _ AMP. 1. 6C　需要一个关于实施 AM 审计(参看下面的 AMA _ EVD 子类)计划进度表的定义、作为 TOE 目标的再次评估的定义，以及所建议的进度表合理性定义。进度表可以用所花费时间的术语定义(如每年一次的 AM 审计)，它们也可以与某一特定的 TOE 新版本相联系。计划的进度表应当考虑在此期间预期的变动，以及从 TOE 评估到建立 AM 计划所花时间内预计的变动。特别地，AM 计划范围外的任何变动将引发再次评估。

AMA _ AMP. 1　保证维护计划

依赖关系：

ACM _ CAP. 2　配置项

ALC _ FLR. 1　基本的缺陷修正

AMA _ CAT. 1　TOE　组件分类报告

开发者行为元素：

AMA _ AMP.1.1D 开发者应当提供一个 AM 计划。

证据的内容和形式元素：

AMA _ AMP.1.1C AM 计划应当包含或引用一个 TOE 的简洁描述，包括它提供的安全功能。

AMA _ AMP.1.2C AM 计划应当标识已认证的 TOE 版本，并引用评估结果。

AMA _ AMP.1.3C AM 计划应当为已认证版本 TOE 引用 TOE 组件分类报告。

AMA _ AMP.1.4C AM 计划应当定义计划应包括的 TOE 变动的范围。

AMA _ AMP.1.5C AM 计划应当描述 TOE 的生命周期，标识任何新版本 TOE 的当前计划，并简洁描述那些具有重要安全影响的预期变动。

AMA _ AMP.1.6C AM 计划应当描述保证维护周期，陈述和证明 AM 审计的计划进度表和下一次 TOE 再次评估的预计日期。

AMA _ AMP.1.7C AM 计划应当标识承担 TOE 开发方安全分析员角色的人员。

AMA _ AMP.1.8C AM 计划应当描述开发方安全分析员如何确保在 AM 计划中文档化或引用的程序得以实施。

AMA _ AMP.1.9C AM 计划应当描述开发方安全分析员如何确保在影响 TOE 安全性的变动分析中所涉及到的开发者全部行为得以正确执行。

AMA _ AMP.1.10C AM 计划应当证明为什么指定的开发方安全分析员非常熟悉安全目标、功能描述和(适当时)TOE 的高层设计，并且熟悉评估结果和所有可用于已认证的 TOE 版本的保证要求。

AMA _ AMP.1.11C AM 计划应当描述或引用即将用于维护 TOE 保证的程序，这至少应包括以下的程序：管理配置、保证证据维护、对影响 TOE 变动的安全影响所作分析的性能，以及缺陷纠正。

评估者行为元素：

AMA _ AMP.1.1E 评估者应当确认所提供的信息满足证据内容和形式的所有要求。

AMA _ AMP.1.2E 评估者应当确认所建议的 AM 审计和 TOE 的再次评估的进度表是可以接受的，并且与所建议的 TOE 变动相一致。

17.2 TOE 组件分类报告(AMA _ CAT)

目的：

TOE 组件分类报告的目的是通过提供一个与安全相关的 TOE(如 TSF 子系统)组件分类来补充 AM 计划。这一分类将作为开发方安全影响分析和随后对 TOE 再次评估的焦点。

组件分级：

本子类仅包含一个组件。

应用注释：

在 AMA _ CAT.1.1 中，术语“最不抽象的 TSF 表示”是指为正在维护的保证级提供的最不抽象的 TSF 表示。例如，如果 TOE 在一个 EAL3 保证级上进行维护，那么最不抽象的 TSF 表示是高层设计，并且下列 TOE 组件必须加以分类：

a) 功能规范中所有可标识的 TSF 外部接口；

b) 高层设计中所有可标识的 TSF 子系统。

因为 AMA _ CAT 要求至少定义两个分类，为了有助于专注开发方的安全影响分析，对于 TSP 实施分类的进一步细分是十分合适的(取决于 TOE 的类型)。例如，TSP 实施的组件可以分为*安全关键*或

安全支持：

a）安全关键的 TOE 组件是那些*直接*负责至少一项在安全目标中定义的 IT 安全功能的实施；

b）安全支持的 TOE 组件是那些对 IT 安全功能实施*不直接*负责的组件（因而不是安全关键的），但是仍然依靠它们来支持 IT 安全功能；这一分类因而可包括两个不同类型的 TOE 组件：

——为安全关键的 TOE 组件提供服务，与正确发挥功能有关的组件；

——不提供任何这样的服务，但仍然要确信没有恶意行为（如引入脆弱性）的组件。

AMA _ CAT. 1. 3C 要求标识所有开发工具，这些工具如果被修改，将会对 TOE 满足其安全目标的保证产生影响（例如用于产生目标代码的编译器）。

AMA _ CAP. 1 TOE 组件分类报告

依赖关系：

ACM _ CAP. 2 配置项

开发者行为元素：

AMA _ CAT. 1. 1D 开发者应当为已认证的 TOE 版本提供 TOE 组件分类报告。

证据的内容和形式元素：

AMA _ CAT. 1. 1C TOE 组件分类报告应当根据其安全相关性，对每个在 TSF 表示中可识别的从最抽象到最不抽象的 TOE 组件进行归类；至少，TOE 组件必须归类为 TSP 实施或非 TSP 实施中的一个。

AMA _ CAT. 1. 2C TOE 组件分类报告应当描述使用的分类方法，这样就能决定如何对引入到 TOE 的新组件进行分类，并且决定在 TOE 或其安全目标变动后何时对现存的 TOE 组件再次分类。

AMA _ CAT. 1. 3C TOE 组件分类报告应当标识在开发中使用的任何工具，如果这些工具被修改，将会对 TOE 满足其安全目标的保证产生影响。

评估者行为元素：

AMA _ CAT. 1. 1E 评估者应当确认所提供的信息满足证据内容和形式的所有要求。

AMA _ CAT. 1. 2E 评估者应当确认 TOE 组件和工具的分类、使用分类的方法是恰当的，并且与已认证版本的评估结果相一致。

17.3 保证维护证据（AMA _ EVD）

目的：

本子类要求的目的是保证开发方已维护了 TOE，并且与 AM 计划相一致。这一目的是通过提供证据说明 TOE 中的保证已经得到维护而达到的，而且这些证据是经过评估者独立校验的。这个检查，术语为“AM 审计”，在 AM 计划的生命期内周期性地执行。

组件分级：

本子类仅包括一个组件。

应用注释：

本子类包含一些与 ACM、ATE 和 AVA 等类中定义的保证要求相类似的证据要求。但是，AM 审计要求评估者检查证据不必与以上那些类的组件要求检查的程度一样；它要求通过抽样来确保保证维护程序已经正确遵循了。

作为 AM 审计的一部分，评估者根据那些与已认证的 TOE 版本相比改变了的 TOE 组件的标识，检验（通过抽样）配置表和安全影响分析是否与 TOE 的当前版本一致。AMA _ EVD. 1. 3C 要求提供证

据表明已遵循了 AM 计划中的保证维护程序。这包括在 AMA _ AMP.1.11C 中提到的所有程序，比如应用有关配置管理的程序的证据、保证证据的维护、安全影响分析的性能以及缺陷纠正。

AMA _ EVD.1.4C 要求的证据包括提供 TOE 当前版本中已识别的缺陷列表。它作为一个独立的要求以示强调，因为在与原评估保证要求相一致的级别上，确保当前版本不包含在 TOE 环境可被利用的任何安全脆弱性，这一点很重要。AMA _ EVD.1.4C 中的列表应包含来自于以下几个方面的脆弱性：

a) AVA _ VLA.1 要求的开发者的分析，或者更高级的组件（如果 TOE 已认证版本要求）；

b) 其他任何被报道的安全缺陷，它们由 ALC _ FLR.1（如果已认证的 TOE 版本要求，则为 ALC _ FLR.2）所要求的缺陷纠正程序进行处理。

AMA _ EVD.1.5E 要求评估者确认功能测试已经在 TOE 当前版本下执行，并且测试的范围和深度同被维持的保证级是相一致的。这个检查是通过对 TOE 当前版本的测试文档进行抽样而得到的。

AMA _ EVD.1　维护过程证据

依赖关系：

AMA _ AMP.1　保证维护计划

AMA _ SIA.1　安全影响分析抽样

开发者行为元素：

AMA _ EVD.1.1D　开发方安全分析员应该为当前 TOE 版本提供 AM 文档。

证据的内容和形式元素：

AMA _ EVD.1.1C　AM 文档应该包含一个配置表及 TOE 中所标识缺陷的列表。

AMA _ EVD.1.2C　配置表应该描述组成当前 TOE 版本的配置项。

AMA _ EVD.1.3C　AM 文档应该提供文档化的或在 AM 计划中引用的程序已被遵循的证据。

AMA _ EVD.1.4C　当前 TOE 版本所标识的脆弱性列表应该能表明，对于每个脆弱性，它不能在预期中的 TOE 环境下使用。

评估者行为元素：

AMA _ EVD.1.1E　评估者应当确认所提供的信息满足证据内容和形式的所有要求。

AMA _ EVD.1.2E　评估者应确认文档化的或在 AM 计划中引用的程序已被遵循。

AMA _ EVD.1.3E　评估者应当确认当前版本的 TOE 的安全影响分析与配置清单相一致。

AMA _ EVD.1.4E　评估者应当确认当前版本的 TOE 的安全影响分析所有改变文档，已写入在 AM 计划所覆盖的改变范围之内。

AMA _ EVD.1.5E　评估者应当确认进行了当前版本的 TOE 的功能测试，其程度与被维护的保证级相一致。

17.4　安全影响分析（AMA _ SIA）

目的：

安全影响分析的目的是确保在 TOE 内保证得到了维护，这是通过认证后由开发者对所有影响 TOE 的变更进行安全影响分析而实现的。

组件分级：

本子类包括两个组件，组件分级基于评估者对开发方安全影响分析检验的程度。

应用注释：

AMA _ SIA.1　要求通过抽样方法来验证开发方的安全影响分析。在一些情况下，认为抽样方法不足以确保当前版本 TOE 中的保证得以维护，而正式的再次评估又被认为没有必要，此时可以使用 AMA _ SIA.2。

本子类的两个组件都需要安全影响分析来标识当前版本 TOE 中所有新的和改动过的组件(与已认证的版本相比而言)。这一信息精确性的检验,或者是在相关的 AM 审计过程中(通过抽样)进行,或是根据 ACM _ CAP 检查配置清单时对 TOE 进行有关的再次评估过程中进行。

AMA _ SIA.1　安全影响分析抽样

依赖关系:

AMA _ CAT.1　TOE 组件分类报告

开发者行为元素:

AMA _ SIA.1.1D　开发方安全分析员应对当前版本的 TOE 提供一个安全影响分析,它覆盖了与已认证版本相比较影响 TOE 的所有修改。

证据的内容和形式元素:

AMA _ SIA.1.1C　安全影响分析应当标识能够导出当前 TOE 版本的已认证的 TOE。

AMA _ SIA.1.2C　安全影响分析应当标识新的和改动过的所有 TOE 组件,它们归属为 TSP 实施类。

AMA _ SIA.1.3C　对于每个影响安全目标或 TSF 表示的变更,安全影响分析应简要描述该修改的影响,以及对较低表示级别的影响。

AMA _ SIA.1.4C　对于每个影响安全目标或 TSF 表示的变更,安全影响分析应当标识所有 IT 安全功能和所有受变更影响 TOE 组件,它们归属为 TSP 实施类。

AMA _ SIA.1.5C　对于导致 TSF 实现表示或 IT 环境的每个变更,安全影响分析应当标识测试证据,此证据表明对保证级的要求来说,TSF 在变动后继续能够得以正确实现。

AMA _ SIA.1.6C　对于在配置管理(ACM)、生命周期支持(ALC)、交付和运行(ADO)以及指导性文档(AGD)保证类中的每个应用的保证要求,安全影响分析应识别任何已经变更的评估交付材料,并简要描述每个修改及其对保证的影响。

AMA _ SIA.1.7C　对于在脆弱性评定(AVA)保证类中的每个应用的保证要求,安全影响分析应当标识那些已经变更和那些未变更的评估交付材料,并对是否更新交付材料所采取的决定给出理由。

评估者行为元素:

AMA _ SIA.1.1E　评估者应当确认提供的信息满足证据内容和形式的所有要求。

AMA _ SIA.1.2E　通过抽样,评估者应当校验安全影响分析以适当详细程度的文档变更情况,并提供适当的理由证明当前版本 TOE 的保证已得到维护。

AMA _ SIA.2　安全影响分析检验

依赖关系:

AMA _ CAT.1　TOE 组件分类报告

开发者行为元素:

AMA _ SIA.2.1D　开发方安全分析员应对当前版本的 TOE 提供一个安全影响分析,它覆盖了与已认证版本相比较,影响 TOE 的所有修改。

证据的内容和形式元素:

AMA _ SIA.2.1C　安全影响分析应当标识能够导出当前 TOE 版本的已认证的 TOE。

AMA _ SIA.2.2C　安全影响分析应当标识新的和改动过的所有 TOE 组件,它们归属为 TSP 实施类。

AMA _ SIA.2.3C　对于每个影响安全目标或 TSF 表示的变更,安全影响分析应简要描述该修改的影响,以及对较低表示级别的影响。

AMA _ SIA.2.4C　对于每个影响安全目标或 TSF 表示的变更,安全影响分析应当标识所有 IT 安全功能和所有受变更影响 TOE 组件,它们归属为 TSP 实施类。

AMA_SIA.2.5C 对于导致 TSF 实现表示或 IT 环境的每个变更，安全影响分析应当标识测试证据，此证据表明对保证级的要求来说，TSF 在变动后继续能够得以正确实现。

AMA_SIA.2.6C 对于在配置管理(ACM)、生命周期支持(ALC)、交付和运行(ADO)及指导性文档(AGD)保证类中的每个应用的保证要求，安全影响分析应识别任何已经变更的评估交付材料，并简要描述每个修改及其对保证的影响。

AMA_SIA.2.7C 对于在脆弱性评估(AVA)保证类中的每个应用的保证要求，安全影响分析应当标识那些已经变更和那些未变更的评估交付材料，并对是否更新交付材料所采取的决定给出理由。

评估者行为元素：

AMA_SIA.2.1E 评估者应当确认提供的信息满足证据内容和形式的所有要求。

AMA_SIA.2.2E 通过抽样，评估者应当校验安全影响分析以适当详细级别的文档所有变更，并提供适当的理由证明当前版本 TOE 的保证已得到维护。

附 录 A
（提示的附录）
保证组件依赖关系的交叉引用

在第 9～15 章和第 17 章的组件中文档化的依赖关系是保证组件之间的直接依赖性。表 A1 总结了直接依赖性和间接依赖性。间接依赖性是对不断引入标识为具有依赖关系的每个组件的依赖性的累积结果。

表 A1 保证组件的依赖关系[a]

组件名	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
AUT. 1-2		3	*1*												*1*											
CAP. 1-2																										
CAP. 3-4			1												1											
CAP. 5			1												2											
SCP. 1-3		3													*1*											
DEL. 1																										
DEL. 2-3		3	*1*												*1*											
IGS. 1-2						*1*					*1*		1													
FSP. 1-4											1															
HLD. 1-2						1					1															
HLD. 3-4						3					2															
HLD. 5						4					3															
IMP. 1-2						*1*	*2*			1	1							1								
IMP. 3						*1*	*2*		1	1	1							1								
INT. 1-2						*1*	*2*	1		1	*1*							*1*								
INT. 3						*1*	*2*	2		1	*1*							*1*								
LLD. 1						*1*	2				1															
LLD. 2						*3*	3				2															
LLD. 3						*4*	5				3															
RCR. 1-3																										
SPM. 1-3						1					*1*															
ADM. 1						1					*1*															
USR. 1						1					*1*															
DVS. 1-2																										
FLR. 1-3																										
LCD. 1-3																										

表 A1(完)

组件名	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
TAT.1-3						*1*	*2*	1		*1*	*1*															
COV.1-3						1					*1*										1					
DPT.1						*1*	1				*1*										1					
DPT.2						*1*	2			1	*1*										1					
DPT.3						*1*	2	2		1	*1*							*1*			1					
FUN.1-2																										
IND.1						1					*1*		1	1												
IND.2-3						1					*1*		1	1							1					
CCA.1-3						2	*2*	2		*1*	*1*		1	1				*1*								
MSU.1-3					1	1					*1*		1	1												
SOF.1						1	1				*1*															
VLA.1						1	1				*1*		1	1												
VLA.2-4						1	2	1		1	*1*		1	1				*1*								
AMP.1		2														1										
CAT.1		2																								
EVD.1																										
SIA.1-2																										

a. 在表 A1 中,左边的栏代表特定组件的组合(只用组件名的后 3 个字母加上组件号或数字范围的标记)。表中的每一个非空的方块表示左边栏目中指定的组件所依赖的一个特定组件,用该列顶部的名字和方块中的数字来标识。粗体的数字表示直接依赖关系,斜体的数字表示间接依赖关系。黑色阴影代表一个组件和它自己有交互性。从 AMA 组件到保证组件的依赖关系都包含在表 A1 中,AMA 内部依赖关系在下面的表 A2 中给出。不存在任何从非-AMA 组件到 AMA 的组件的依赖关系,所以表 A1 没有代表 AMA 子类的列。

表 A2 AMA 内部依赖关系

AMA 组件名	AMP	CAT	EVA	SIA
AMP.1		1		
CAT.1				
EVD.1	1	*1*		1
SIA.1-2		1		

附 录 B
（提示的附录）
EAL 和保证组件的交叉引用

表 B1 给出了评估保证级(EAL)与评估类、子类和组件之间的关系。

表 B1 评估保证级汇总

保证类	保证子类	评估保证级(EAL)依据的保证组件						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
配置管理	ACM _ AUT				1	1	2	2
	ACM _ CAP	1	2	3	4	4	5	5
	ACM _ SCP			1	2	3	3	
交付和运行	ADO _ DEL		1	1	2	2	2	3
	ADO _ IGS	1	1	1	1	1	1	1
开发	ADV _ FSP	1	1	1	2	3	3	4
	ADV _ HLD		1	2	2	3	4	5
	ADV _ IMP				1	2	3	3
	ADV _ INT					1	2	3
	ADV _ LLD				1	1	2	3
	ADV _ RCR	1	1	1	1	2	2	3
	ADV _ SPM				1	3	3	3
指导性文档	AGD _ ADM	1	1	1	1	1	1	1
	AGD _ USR	1	1	1	1	1	1	1
生命周期支持	ALC _ DVS			1	1	1	2	2
	ALC _ FLR							
	ALC _ LCD				1	2	2	3
	ALC _ TAT				1	2	3	3
测试	ATE _ COV		1	2	2	2	3	3
	ATE _ DPT			1	1	2	2	3
	ATE _ FUN		1	1	1	1	2	2
	ATE _ IND	1	2	2	2	2	2	3
脆弱性评定	AVA _ CCA					1	2	2
	AVA _ MSU			1	2	2	3	3
	AVA _ SOF		1	1	1	1	1	1
	AVA _ VLA		1	1	2	3	4	4